

A large, thick, orange abstract line that starts from the left edge, curves upwards and to the right, then loops back down and to the left, forming a large, irregular, teardrop-like shape that frames the title text.

ProtectDrive

User Manual

Document Revision A19



THIS PAGE INTENTIONALLY LEFT BLANK

Preface

Copyright

No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise without the prior written permission of:

Eracom Technologies
28 Greg Chappell Drive
Burleigh Heads, Queensland 4220
AUSTRALIA

National (07) 5593-4911
International +61 75593-4911
FAX (07) 5593-4388
Website: www.eracom-tech.com

Copyright © Eracom Technologies 2006, all rights reserved

All trademarks are acknowledged as the property of their respective owners.

Disclaimer

Eracom makes no representations or warranties with respect to the contents of this manual and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Eracom reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation on Eracom to notify any person or organization of such revision or changes.

Publication Improvements

Eracom invites constructive comments on the contents of this manual. These comments, together with your personal and/or Company details, should be sent to Development Support at the above address. Alternatively you can e-mail us at support@safenet-inc.com.

Revision Incorporation Certificate

Revision	Release Date	Description
A0	June 2002	Initial Release
A1	September 2, 2002	Rev 1.0
A2	September 18, 2002	Rev 1.1
A3	December 13, 2002	Remote Password Recovery.
A4	July 2003	New features for 6.0.0 release
A5	July 22, 2003	Print anomaly corrections
A6	August 29, 2003	Add auto-logon functionality
A7	September 17, 2003	Add token authentication and new 6.1.0 features
A8	December 17, 2003	Addition of 3DES and NT support
A9	January 7, 2004	Removed Upgrade support for 6.1.0
A10	March 2004	Updated to meet requirements of CC Evaluation and PD V7.0.2
A11	June 2004	Separate revision for CC evaluation of ProtectDrive 7.0.2
A12	June 2004	Updated for ProtectDrive 7.1.0
A13	October 2004	Separate revision for CC evaluation of ProtectDrive 7.0.3 derived from Rev A11 Updated version information to V7.0.3 Reformatted Pages, TOC, Header and Footer
A14	January 10, 2005	Derived from revision A12 Updates for ProtectDrive 7.2.0 Updates to screen shots Ability to boot from floppy after pre-boot logon removed Details regarding defragmentation removed
A15	May 2005	Various Bugs fixed
A16	July 2005	Reserved for Japanese translation
A17	August 2005	Changes per PD 7.2.3
A18	February 2006	Single Sign-On chapter added.
A19	March 2006	Changed for ProtectDrive 7.2.4 - Changed registration process - Certificate selection feature

Important

The following user manuals cover the full functionality of ProtectDrive:

User Manual



Network Installation Guide



Table of Contents

Preface.....	i
C H A P T E R 1 The Requirement for Security	1
C H A P T E R 2 Additional Guidance Regarding Security.....	3
<i>Evaluated Versions of ProtectDrive.....</i>	<i>3</i>
<i>Guidance for Users of ProtectDrive</i>	<i>3</i>
Further Reading Relevant to the CC Certification	3
<i>Delivery Procedures.....</i>	<i>4</i>
<i>Product Identification</i>	<i>5</i>
Before Installation:	5
After Installation.....	5
<i>Organizational Requirements</i>	<i>6</i>
Connections to Outside Systems.....	6
Guidance.....	6
Tampering.....	6
Training	6
Tokens	6
Users.....	6
USB and other I/O Devices	6
<i>Guidance for the Operating System Configuration.....</i>	<i>7</i>
General	7
Password Policy.....	7
Screen Lock Feature	8
<i>Information Relevant to Administrators of ProtectDrive.....</i>	<i>8</i>
Operating Systems.....	8
Evaluated items.....	8
Encryption Algorithm.....	8
Show Disk Not Fully Encrypted Warning	8
Automatic Pre-boot Authentication	9
Show Unsuccessful Logon Warnings	9
Access Control.....	9
C H A P T E R 3 Features and Functions	11
<i>Strong Authentication.....</i>	<i>11</i>
Two-Factor Authentication.....	11
Password Authentication	11
<i>Diskette Drive Access.....</i>	<i>12</i>
<i>Port Access Permissions</i>	<i>12</i>
<i>Fixed Disk Accessibility</i>	<i>12</i>
<i>Multi-user Support</i>	<i>12</i>
<i>System Performance.....</i>	<i>12</i>
<i>Application Performance</i>	<i>13</i>
<i>System Backup and Recovery.....</i>	<i>13</i>
<i>Multiple Boot Configurations.....</i>	<i>13</i>
C H A P T E R 4 Considerations and Restrictions.....	15
<i>Non-Removable Hard Disk Drives.....</i>	<i>15</i>
<i>Iomega ATAPI Internal Zip Drives and the Like</i>	<i>15</i>
<i>Floppy Disk Drives.....</i>	<i>16</i>
<i>SCSI Drives</i>	<i>16</i>
<i>Drives Accessed using DOS drivers or TSRs</i>	<i>16</i>
<i>Error Messages</i>	<i>16</i>
<i>File Safety.....</i>	<i>17</i>

<i>Number of Users</i>	17
<i>Password Length</i>	17
<i>User Name Length</i>	17
C H A P T E R 5 Incompatibilities	19
<i>Windows Folder Compression</i>	19
<i>Protecting System Files from Corruption</i>	19
<i>Windows System Restore</i>	19
<i>Multiple Boot Systems</i>	19
<i>Fixed Disk Formatting & Partition Changes</i>	20
<i>Master Boot Record</i>	20
<i>Windows 2000/XP Disk Management Program</i>	20
<i>Windows 2000/XP User Manager Shortcuts</i>	20
<i>Windows Fast User Switching</i>	20
<i>Windows Username Compatibility</i>	21
<i>Version Specific Restrictions</i>	21
C H A P T E R 6 Installation	23
<i>Multiple Boot System Preparation</i>	23
<i>Installation Requirements</i>	23
<i>Before Installation</i>	24
<i>Choosing the installing user account</i>	25
<i>Registration disk and recovery disk</i>	26
Registration disk	26
Recovery disk	27
Creating your own recovery keys	27
<i>Phase 1. Starting the Installation Process</i>	28
<i>Phase 2. Completing the Installation</i>	29
Configuration Options	30
Types of Users	31
Authentication Settings.....	32
Certificate Selection.....	35
Domain Users and Groups	36
One-Time Pre-Boot Password	37
Default Disk/Port Permissions.....	37
Disk Encryption Algorithm Options	37
Multi-Boot Manager	38
Installation Progress.....	38
<i>Installation of Server Components</i>	39
C H A P T E R 7 Single Sign-On Management	43
<i>The Single Sign-On Assistant</i>	43
Overview	43
Accessing the Single Sign-On Assistant.....	44
Windows Authentication	44
Post-Authentication Accounts	44
<i>RSA SOM Support</i>	44
Overview	44
Implementation.....	45
Considerations	45
<i>Third Party Product Support</i>	45
Overview	45
Support for Third-Party GINAs	46
Support for Third-Party Accounts.....	46
<i>Novell Client Support</i>	46
Overview	46
Implementation.....	46

Known Issue	47
Administrative Procedures.....	47
Configuration after ProtectDrive Installation Over an Existing System	47
Configuration after Installing Additional Software to the ProtectDrive System	47
Changing chained GINA	48
Setting GINA Configuration.....	48
Creating a Post-Authentication Account.....	49
Modifying a Post-Authentication Account	51
Removing a Post-Authentication Account.....	52
Creating a Post-Authentication Account Field.....	52
Modifying a Post-Authentication Account Field	53
Removing a Post-Authentication Account Field.....	54
Exporting SSO Settings	54
C H A P T E R 8 Upgrading ProtectDrive.....	55
<i>Upgrading the Recovery Tools.....</i>	<i>55</i>
<i>Upgrading</i>	<i>56</i>
Network Upgrades	56
<i>Upgrading a ProtectDrive version earlier than 7.2.2.....</i>	<i>56</i>
Authentication Settings.....	56
Default Disk/Port Permissions.....	57
Upgrading from PCVault 5.12.4	57
<i>Restoring ProtectDrive</i>	<i>58</i>
<i>Removing the Upgrade Archive</i>	<i>58</i>
C H A P T E R 9 Uninstalling ProtectDrive	59
<i>Normal Uninstall.....</i>	<i>59</i>
<i>Problems with Uninstall.....</i>	<i>59</i>
C H A P T E R 10 Logging On	61
<i>Pre-Boot Authentication.....</i>	<i>61</i>
Token or Smart Card Logon	62
Password Logon	64
<i>Windows Logon.....</i>	<i>64</i>
<i>First Time Logon.....</i>	<i>64</i>
New User Introduction by Existing Administrator	65
New User Introduction in the Absence of an Existing Administrator	65
<i>Unsuccessful Logon.....</i>	<i>66</i>
<i>Successful Logon.....</i>	<i>66</i>
<i>Unsuccessful Logon Attempt Warnings.....</i>	<i>66</i>
<i>Diskette Boot</i>	<i>67</i>
<i>Token Removal</i>	<i>67</i>
C H A P T E R 11 Configuring ProtectDrive	69
<i>After Installation</i>	<i>69</i>
<i>Advanced Configuration Options.....</i>	<i>69</i>
<i>User ShellTab.....</i>	<i>70</i>
Authentication Tab	71
<i>Disk Encryption Tab.....</i>	<i>73</i>
C H A P T E R 12 ProtectDrive and Networking	79
<i>Network Installation.....</i>	<i>79</i>
<i>Local and Domain Accounts</i>	<i>79</i>
<i>Server-Side User Management.....</i>	<i>80</i>
C H A P T E R 13 Recovery Administration.....	81
<i>Remote User Key Recovery.....</i>	<i>82</i>

<i>Password Fallback for Token Users</i>	<i>82</i>
<i>New User Introduction.....</i>	<i>83</i>
<i>Remote Recovery Administration Console.....</i>	<i>83</i>
Enter Challenges.....	84
C H A P T E R 1 4 Recovery Tools.....	85
<i>Location of Recovery Tools.....</i>	<i>85</i>
<i>Using Recovery Tools.....</i>	<i>85</i>
Using Recovery Data Files	86
<i>Recovery Tools</i>	<i>86</i>
<i>RMBR.EXE.....</i>	<i>86</i>
<i>DECDISK.EXE.....</i>	<i>88</i>
<i>DISPEFS.EXE.....</i>	<i>90</i>
<i>BACKUP.EXE.....</i>	<i>90</i>
<i>PDUSERDB.EXE.....</i>	<i>92</i>
C H A P T E R 1 5 Encrypt-Decrypt Hard Drives.....	94
<i>Using Crypdisk.....</i>	<i>94</i>
<i>Encryption Algorithm Selection</i>	<i>95</i>
DES Cipher.....	95
Triple DES Cipher	95
IDEA	96
AES	96
<i>Disk Encryption Security Warning.....</i>	<i>96</i>
Security Warning.....	96
<i>Drive Selection</i>	<i>97</i>
<i>System Areas Only.....</i>	<i>97</i>
<i>Priority Selection.....</i>	<i>97</i>
Priority - Low	98
Priority - Normal	98
Priority - High.....	98
<i>Encryption.....</i>	<i>98</i>
<i>Decryption.....</i>	<i>99</i>
<i>List View.....</i>	<i>99</i>
<i>Command Line Options.....</i>	<i>100</i>
Determining the Encryption Status of a Disk.....	100
<i>Backing up.....</i>	<i>101</i>
C H A P T E R 1 6 User Management	103
<i>User Database Management.....</i>	<i>103</i>
<i>Introducing New Users.....</i>	<i>103</i>
<i>User Privileges.....</i>	<i>104</i>
Administrators	104
End Users.....	104
<i>User Properties</i>	<i>104</i>
<i>Usernames.....</i>	<i>105</i>
<i>Privileges and Access Permissions</i>	<i>105</i>
<i>Diskette Permissions</i>	<i>106</i>
C H A P T E R 1 7 Passwords.....	107
<i>System Chosen Passwords</i>	<i>107</i>
<i>User Chosen Passwords.....</i>	<i>107</i>
<i>Password Security.....</i>	<i>107</i>
<i>Password Strength Enforcement</i>	<i>107</i>
<i>Choosing Passwords</i>	<i>108</i>

<i>A List of Don'ts for Choosing Passwords:</i>	108
<i>A List of Dos for Choosing Passwords:</i>	108
<i>Password Changing Restrictions</i>	108
<i>Password Ageing</i>	109
<i>Assigning Passwords to New Users</i>	109
<i>Password History</i>	109
<i>Lockout Feature</i>	109
<i>Password Attacks</i>	109
C H A P T E R 18 Automatic Pre-Boot Authentication	111
<i>Using the SetAutoPBA Utility</i>	111
<i>Amending the Windows Registry</i>	111
<i>Setting Up Automatic Pre-Boot Authentication</i>	113
C H A P T E R 19 Token Initialisation	115
<i>Setting up Windows Smart Card Logon</i>	115
<i>Installing the Smartcard Runtime Environment</i>	116
Working with the Microsoft Management Console	116
Setting Up Smart Card Enrollment	117
Issuing Logon Tokens.....	118
C H A P T E R 20 The Multiple Boot System	120
<i>Introduction</i>	120
<i>Limitations to Version 7.2.*</i>	120
<i>Design Considerations</i>	120
<i>Operating Systems</i>	121
<i>File Systems</i>	122
<i>Sharing Data</i>	122
<i>Operating System Installation</i>	122
<i>Installation</i>	122
Disk Management Tools	122
Partitioning	123
Labeling Partitions.....	123
Other Operating Systems	123
Pre-Installation Verification	124
<i>Installing</i>	124
<i>Uninstalling ProtectDrive</i>	126
C H A P T E R 21 ACS Error Messages and System Recovery	127
<i>Error message identification</i>	127
<i>Standard Recovery Procedure</i>	131

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1

The Requirement for Security

The widespread use of PCs and laptops for business, home, and entertainment makes them an attractive and convenient warehouse of information. However, their increasing capacity makes the owner vulnerable to financial loss if the information they contain is destroyed, tampered with, or stolen. In many countries, Privacy Legislation makes the securing of certain types of confidential data mandatory.

It is not always possible to lock a PC in a room when its user is absent. Consequently, other people may have access to its information. This may include people who are not authorized to observe confidential or private data contained in that computer.

ProtectDrive is Eracom Technologies' encryption software, designed to provide protection for PCs and laptop computers. ProtectDrive is fully transparent in use and requires no knowledge of encryption by the user.

With ProtectDrive installed, access to a PC is only available by logging on with a valid username and password or token and PIN. As long as this logon information remains confidential, access to the PC will be denied to any unauthorized person.

If a system is stolen or lost, the information contained on the hard disk remains secure due to the encryption techniques used.



THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2

Additional Guidance Regarding Security

Evaluated Versions of ProtectDrive

This chapter provides important guidance to users of evaluated versions of ProtectDrive. Evaluation of ProtectDrive is based on assumptions contained in a Security Target for the evaluation.

The Security Target describes the basis of the evaluation including:

- threats that the security claims of ProtectDrive are designed to counter
- environmental and organizational assumptions required to support the security claims
- constraints to the configuration of ProtectDrive required to support the security claims

When relying on an evaluated version of ProtectDrive, users should follow the recommendations in this chapter, refer to the evaluation Security Target and refer to the Certification Report for guidance on use of the evaluated version of ProtectDrive.

The Security Target and the Certification Report can be found at the Common Criteria Evaluated Products List (EPL). Both the Security Target and Evaluation Technical Report are available online upon completion of an evaluation.

This list, for ProtectDrive, may be found at:

http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html

Guidance for Users of ProtectDrive

Further Reading Relevant to the CC Certification

The following documents should be read in conjunction with this manual:

- ProtectDrive Security Target
- ProtectDrive Certification Report
- Release Notes included on the distribution CD
- README.TXT included with the distribution CD

Users are reminded that evaluated versions of ProtectDrive are based on assumptions contained in the evaluation Security Target. In particular, the following chapters should be read:

- Chapter 3 – Assumptions; and
- Chapter 4 - Security Objectives for the Environment.

These chapters describe the responsibility of users and detail requirements needed to ensure that ProtectDrive product is used and administered securely.

Delivery Procedures

Standard commercial practice is used for the packaging and delivery of ProtectDrive. Registered copies of ProtectDrive are distributed in a shrink-wrapped package that comprises:

- a CD-ROM containing the ProtectDrive software, user manual, Release Notes, and a **README.TXT** notice
- a diagnostic floppy disk holding licence information
- a licence certificate
- a support agreement certificate (if a support agreement has been purchased) and
- a packing list

On receipt of a delivery, you should:

- Check the delivery for any signs of tampering (e.g., shrink wrap package open or damaged)
- Check the packing list to ensure all items are correct and that the customer purchase order number and the Eramcom Technologies sales order number are consistent with the delivery

On opening the package, you should verify the product identification by checking the product version number, which is printed on the CD-ROM and on the packaging.

If there are any signs of tampering or any inconsistencies with the delivery or the product version, then you should immediately notify Eramcom Technologies.

Product Identification

To ensure that the copy of ProtectDrive you have is authentic and is the correct version you should:

Before Installation:

- As noted above, under “Delivery Procedures”, if the product or its packaging shows signs of tampering when it is received, you should notify Eracom Technologies for advice before using the product.
- Check the product version number on the CD volume label. You should ensure that the volume label identifies the version as **PD x.yy.zz**, where x.yy.zz is the ProtectDrive version number (e.g., PD 7.02.02). If you are using an evaluated version of ProtectDrive, ensure that the version you are installing matches the version listed in the Evaluated Products List.
- If installing ProtectDrive from an electronic archive, ensure that the file name is **pd_x_yy_zz**, where x_yy_zz is the version number.
- Ensure that the files README.TXT and Release Note on the distribution CD-ROM refer to the product version being used.
- All files in the ProtectDrive installation package are electronically signed. The file **PD_x_yy_zz.sig** contains the signatures of all files contained in the installation package. To verify the integrity of the installation package, download and use the **File Verify** utility from Eracom Technologies Internet site.

<http://www.eracom-tech.com/fileverify>

Instructions for using the File Verify utility may be found in the File Verify Technical Bulletin, which is available from the same location as the File Verify utility. The File Verify utility may also be obtained by contacting the Eracom Technologies support section.

After Installation

Verify the version number of ProtectDrive after installation by starting the ProtectDrive About application. Navigate to the following directory:

Start|Programs|ProtectDrive|About ProtectDrive

Verify that the version number displayed matches the expected version number of the installed software.

Organizational Requirements

Connections to Outside Systems

Those responsible for management of the systems in which ProtectDrive is used must ensure that no connections are provided to outside systems that would undermine the security features of ProtectDrive.

Guidance

Guidance should be provided that details the delivery, installation, configuration, administration and operation of ProtectDrive within an organization.

Tampering

The system on which the product is installed must have features that detect physical tampering and provide a clear indication to users that tampering has occurred. Users must be able to check the system for indications of tampering regularly.

Training

All users of ProtectDrive, with administrator privileges, must receive sufficient training to enable them to administer ProtectDrive securely.

Users of ProtectDrive with administration privileges are responsible for implementing guidance that ensures ProtectDrive is installed, configured, administered and operated in a secure manner consistent with the evaluated configuration.

Tokens

Smartcards or Tokens used with ProtectDrive, for authentication, must provide an adequate level of security to protect authentication information and perform the functions required by ProtectDrive. This security may be gained through assurance of the Smartcard or Token or a combination of Smartcard or Token assurance combined with organizational procedures.

Users

Users of ProtectDrive must receive sufficient guidance and training to be able to fulfill their duties.

USB and other I/O Devices

I/O devices, such as USB and Firewire ports for example, may pose a risk that protected information could be accidentally sent to a device without adequate protection. If the risk posed by I/O devices is unacceptable then an organization policy should be used to specify and restrict the use of these I/O devices. If the risk is unacceptable even through procedural policy then the I/O devices should be disabled at the operating system as a part of the system configuration. General

users should not have system privileges that would enable them to change the status of an I/O Device.

ProtectDrive currently manages secure use of Floppy Disk, Serial Ports (COM) and Parallel Port (LPT). Future releases of ProtectDrive may provide secure operation of other I/O devices.

Guidance for the Operating System Configuration

General

ProtectDrive provides protection of information through pre-boot authentication and access control of peripheral devices combined with hard disk encryption. Once access is gained to a computer (by correct user authentication) the user is then responsible for ensuring that the computer is treated in accordance with organizational security policies for the level of information available.

Administrators of ProtectDrive are responsible for ensuring that the underlying operating system is correctly configured and complies with organizational security policies.

If the computer on which ProtectDrive is installed is a part of a network domain then the domain security policies must be correctly configured and comply with organizational security policies.

Password Policy

The operating system password policy must be configured in accordance with organizational policies and be consistent with ProtectDrive requirements. The following minimum settings should be used:

Enforce Password History	7 passwords
Maximum Password Age	In accordance with organizational policy
Minimum Password Age	1 day or greater if required by organizational policy
Minimum Password Length	6 characters or greater if required by organizational policy
Passwords Must Meet Complexity Requirements	Enabled
Store Password Using Reversible Encryption	Disabled

Screen Lock Feature

The operating system screen lock feature must be enabled and configured in accordance with organisational requirements. If the screen lock feature is not enabled and configured correctly, ProtectDrive security features may be subverted.

Information Relevant to Administrators of ProtectDrive

Operating Systems

Evaluated versions of ProtectDrive are tested on specific version of operating systems. For example:

- Microsoft Windows 2000 Professional, 5.00.2195 Service Pack 4
- Microsoft Windows XP Professional 5.1.2600 Service Pack 2 Build 2600.

The operating systems for which ProtectDrive is evaluated are listed in the evaluation Security Target.

While the product will operate with a wider range of service packs and builds, if you wish to use it in its evaluated configuration you should only use it on those specified above.

Evaluated items

Note that the “Server Edition” of ProtectDrive has not been evaluated, nor has the “Multiple Boot Manager” functionality. Furthermore, only the “Registered Product” has been evaluated.

The evaluation does allow for the installation of ProtectDrive over a network, so this manual should be read in conjunction with the network installation manual by those administrators that will be performing the installation in that way.

Encryption Algorithm

To comply with Government advice, only the AES and Triple-DES encryption algorithms have been evaluated, and one of these algorithms should be selected during installation. This will ensure that the correct components are installed and the choice of algorithms available for initial encryption will be limited to AES and 3DES.

Show Disk Not Fully Encrypted Warning

It is strongly recommended that this option be set ON in the evaluated configuration so that users are advised if the disk they are working on is not completely encrypted. When set to ON, the warnings will be displayed for all users.

Automatic Pre-boot Authentication

This option must be used with caution, and strictly as directed in the relevant chapter of this User Guide.

Show Unsuccessful Logon Warnings

This should be set on in the evaluated configuration so that the user is warned of unsuccessful logons.

Access Control

ProtectDrive offers a number of access control options—User ID and Password, Token and PIN, and password recovery and fallback options, as well as new user introduction.

Evaluated versions of ProtectDrive may not include all access control options. When using an evaluated version of ProtectDrive users should refer to the evaluation Security Target to determine which options form part of the evaluated version. Only those access control options that form a part of the evaluated version of ProtectDrive should be enabled.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3

Features and Functions

Strong Authentication

ProtectDrive offers strong authentication through two-factor or password authentication before the operating system is loaded.

Two-Factor Authentication

Two-factor authentication requires users to authenticate by presenting something they **have** and something they **know**. ProtectDrive uses tokens and PINs to authenticate legitimate users. The cryptographic and safe key storage capabilities of the token provide high levels of data protection. ProtectDrive integrates seamlessly with the Windows smart card logon support and does not require any additional token or user management infrastructure.

See CHAPTER 19 for more information on the use of tokens or smart cards with ProtectDrive.

Password Authentication

The strength of passwords used will depend on the situation. In a high-risk situation, ProtectDrive and Windows provide mechanisms to raise the password strength requirements of users. Windows password strength requirements are defined through the “Password Policy”. Since the Windows and ProtectDrive requirements overlap and can potentially conflict, the ProtectDrive password strength checks can be disabled at installation.

Read CHAPTER 17 for more information on selecting and using passwords.

Diskette Drive Access

Diskette drive Read/Write access for every user of the PC can be configured on an individual basis. Read access restriction is useful when it is desirable to control the import of new or unauthorized software.

Write access restriction is useful to control the export (copying) of information or software from the PC. Write access restrictions also imply format access restrictions and prevent users from accidentally or otherwise erasing information stored on floppy diskettes.

Default diskette access permissions, defined during installation, are initially given to each user added to the ProtectDrive user database.

They can be re- assigned during installation by using the Configuration Response File, or after installation by using ProtectDrive User Management applications.

Port Access Permissions

COM and LPT port access permissions are selectable for all users. Default port permissions, defined during installation, are initially given to each user added to the ProtectDrive user database. Port access permissions can be re-assigned to a user during installation by using the Configuration Response File, or after installation by using ProtectDrive User Management applications.

Fixed Disk Accessibility

ProtectDrive uses advanced cryptographic techniques to secure the fixed disk(s). Therefore, if a vital software component of ProtectDrive is removed, the fixed disk(s) will be inaccessible because all components need to be present for correct operation.

Multi-user Support

A built-in Administrator, with a maximum of 200 other users, is permitted. ProtectDrive allows an Administrator complete freedom over how to best control access to the system and its information. Therefore, ProtectDrive can be effectively used in situations ranging from the home environment through to large offices where many users require access to the PC.

System Performance

During operations with ProtectDrive installed, the system is required to encrypt/decrypt in real time. The cipher speed is directly related to the PC processor speed, the size of the disk cache, and the fixed disk speed. The time it takes ProtectDrive to carry out cipher operations on disk data is many times faster than the access time of the fixed disk itself.

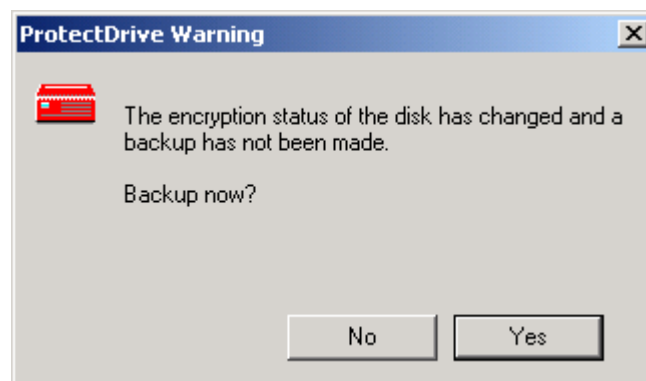
High performance pipelined encryption operations are a feature of ProtectDrive. This means that as the operating system presents multiple disk I/O requests, the cryptographic operations of each request are carried out during the latency period of the following/previous disk I/O operation. This results in a very low discernible overhead for the cryptographic operation.

Application Performance

Most applications, such as Word Processors, spend much of their time processing data that is in the computer's memory and they infrequently access the fixed disk. With these applications, it will be nearly impossible to detect the presence of ProtectDrive in operation. Other applications, such as CHKDSK, spend most of their processing time accessing the fixed disk. On such disk intensive applications, slight performance degradation may be noticed.

System Backup and Recovery

ProtectDrive recovery tools enable system recovery using backed up ProtectDrive data files. If the backup option is selected during installation or turned on after installation, ProtectDrive will display the following dialog prompting the user to perform a backup each time the encryption status of the drives changes.



These files can then be used to fully recover an encrypted system should the ProtectDrive embedded file system (EFS) become corrupt.

Refer to CHAPTER 14 for details on the ProtectDrive recovery tools.

Multiple Boot Configurations

ProtectDrive supports multiple booting to more than one drive by providing a Boot Manager. The Boot Manager menu will run before the pre-boot logon on component of ProtectDrive. It is important that the process for building a multiple boot system outlined CHAPTER 20 be followed.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4

Considerations and Restrictions

Non-Removable Hard Disk Drives

ProtectDrive does not support the addition or removal of non-removable hard disk drives after ProtectDrive has been installed. Therefore, all non-removable hard drives you wish to use on the system with ProtectDrive must be present for the duration of the ProtectDrive installation process.

Non-removable hard drives added after ProtectDrive has been installed will not be able to be accessed. If disks are added or removed after the software's installation, disk corruption may occur.

All partitions on non-removable hard drives can be encrypted at the Administrator's discretion and diskette access privileges are not applied.

The IDE standard supports up to four drives. More can be supported using a SCSI interface. There is no practical limit on drive capacity.

A total of 24 separate partitions can be encrypted; however, in practice this number will be less, due to the presence of removable drives, like floppy drives, CD drives, USB memory drives, or network mapped drives.

ProtectDrive supports the FAT16, FAT32, NTFS4, and NTFS5 file systems.

When slave drives are present, they may be turned off after installation. However, it must be remembered that:

- Slave drives may not be substituted or swapped after ProtectDrive installation.
- Encrypted slave drive partitions will have to be decrypted for uninstallation.

Iomega ATAPI Internal Zip Drives and the Like

The same restrictions as for non-removable hard disk drives apply to internal ATAPI Zip drives. They cannot be added or removed after installation. This does not apply to external Iomega drives.

Note: Zip drives cannot be encrypted.

Floppy Disk Drives

ProtectDrive supports addition and removal of 3.5" floppy disk drives after ProtectDrive has been installed. Any floppy drive can be removed after ProtectDrive's installation.

The addition of floppy drives is dependent on an installation option. By default, addition of floppy drives will not be permitted. If addition of floppy drives is required, it must be configured during installation.

If addition of floppy drives is not configured, the number of accessible drives is limited to the number of drives present during installation. If floppy drives are added after ProtectDrive installation, the operating system's drive initialization sequence determines which drive(s) will be accessible. Therefore, a drive added after installation may have access, but a drive present during installation may not have access if the additional drive is initialized before the original drive.

Drives present at installation may be replaced with another drive of the same type and it will have access.

Floppy drives cannot be encrypted and diskette access privileges will be enforced.

SCSI Drives

SCSI drives are supported; however, Administrators should prepare a DOS boot disk in the event that these disks have to be decrypted using the CDSK recovery utility.

Drives Accessed using DOS Drivers or TSRs

Under DOS (if booting from a DOS diskette), ProtectDrive only sees drives accessible using the BIOS. ProtectDrive does not see drives accessible via a DOS driver or TSR, which means that these drives can be used without intervention from ProtectDrive.

Error Messages

If, for some reason, an abnormal situation arises, ProtectDrive displays an error message.

WARNINGS: Warning messages indicate that an error has possibly occurred. However, the system attempts to continue operating. In some cases, the warning may just be a precursor to a more serious message.

ERRORS: Error messages indicate that an error has occurred. This may result in some portion of the system ceasing to operate. The remainder of the system continues operating, if possible.

FATAL ERRORS: Fatal error messages warn that a destructive fault has occurred. The system cannot continue to function.

Refer to CHAPTER 21 for more information on ACS error messages.

If you fail to understand how to correct the fault, contact your ProtectDrive support person for advice.

File Safety

ProtectDrive encryption drivers and some dynamic link libraries are stored in the Windows system area of the disk. While the fixed disk is encrypted, the Transparent Encryption Driver, TED.SYS must never be removed from the system. In an encrypted system, removal of this driver will, at best, reduce system performance and, at worst, render the disk effectively corrupt.

The removal of other ProtectDrive files will compromise the security of the system rendering ProtectDrive ineffective. Most ProtectDrive files are stored in the SECURDSK directory of your first fixed disk (i.e. C:\SECURDSK). Most of these files are marked read-only, System, and Hidden to prevent accidental erasure or alteration. Any tampering, deletion and moving can cause the ProtectDrive system to fail and may result in data loss.

Number of Users

ProtectDrive can support a maximum of 200 users per workstation.

Password Length

Minimum of 6 and a maximum of 20 characters (alphanumeric).

User Name Length

ProtectDrive supports user names with a length between 1 and 20 characters.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5

Incompatibilities

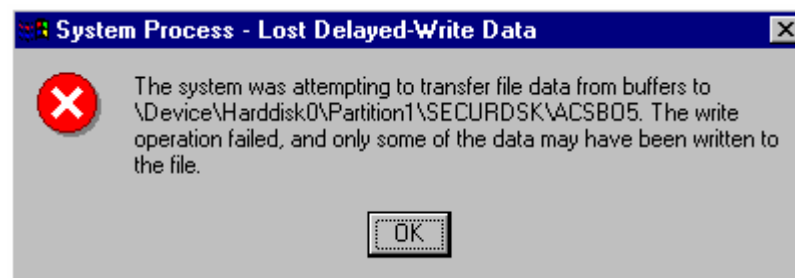
Windows Folder Compression

The C:\SECURDISK directory must not be compressed. Otherwise, its contents are not available to ProtectDrive before the operating system starts and the system will not boot.

On installation, ProtectDrive ensures that the C:\SECURDISK directory is not compressed. If the entire C: drive is compressed, the installer disables this attribute for the C:\SECURDISK directory only. Enabling compression for the C:\SECURDISK or its parent folder can prevent a system from booting.

Protecting System Files from Corruption

To protect itself from corruption, ProtectDrive write-protects all sectors on the disk that are occupied by the ProtectDrive system. Normal access to the disk should never write to these sectors and, thus, there will be no problem. If, however, a write attempt is made to one of these sectors, a Windows screen appears with a warning message:



If this occurs while running a certain application, the application should simply fail. This application is not compatible with ProtectDrive.

If disk write errors persist, consult Eracom support for advice.

Windows System Restore

ProtectDrive installations cannot be undone using the Windows System Restore mechanism. The System Restore feature can be used to revert to restore points created after ProtectDrive installation.

Multiple Boot Systems

The dual boot configuration from one partition as described in the Windows 2000 documentation is not supported. Please refer to CHAPTER 20 for a detailed description of setting up a multiple boot system with ProtectDrive.

Fixed Disk Formatting & Partition Changes

ProtectDrive does not allow partition configuration changes or formatting of the primary partition of the first hard disk, as data loss will occur. Re-formatting the fixed disk when ProtectDrive is installed may be possible with some vendor-specific low-level format utilities.

Always uninstall ProtectDrive prior to a low-level format.

Disk management utilities, such as Partition Magic, can safely be used to set up drives before installation. However, these programs should be removed from the system prior to the installation of ProtectDrive to guard against inadvertent use once ProtectDrive is installed.

Operations such as partition resizing, reposition, conversion, and masking active will result in loss of data.

Master Boot Record

ProtectDrive manipulates the Master Boot Record and verifies its integrity on start-up. Other software, such as boot managers, manipulate the boot record and are incompatible with ProtectDrive. Ensure you are not running software that manipulates the Master Boot Record.

Windows 2000/XP Disk Management Program

Note: Partition Changes cannot be made after ProtectDrive is installed.

The ProtectDrive write protection of the boot sector will prevent most of the Disk Management tasks from succeeding. This includes removing and creating partitions, including Disk Mirroring changes. If you need to perform any of these tasks, uninstall ProtectDrive first.

Windows 2000/XP User Manager Shortcuts

If you have any pre-existing shortcuts to either the User Manager or User Manager for Domains before you install, then these will not provide ProtectDrive user management. Delete the shortcuts prior to installation.

Windows Fast User Switching

ProtectDrive does not support this feature, which is available on Windows computers that are not member of a network domain. After ProtectDrive installation the Windows' **Welcome** screen that allows fast user switching is no longer available.

Windows Username Compatibility

The single sign-on facility provided by ProtectDrive requires that usernames and passwords for both Windows and ProtectDrive be shared.

The only added restriction of ProtectDrive usernames and passwords is that all characters must be printable ASCII or ANSI characters (i.e., printable single byte characters in the range 0-255). This includes all English and most European characters.

The ProtectDrive Setup Program will verify Windows usernames for ProtectDrive compatibility.

Version Specific Restrictions

Specific restrictions may be applicable to your version of ProtectDrive. View the README.TXT file on the installation CD for version specific information.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 6

Installation

Note: When deploying ProtectDrive on systems containing multiple hard disks, **disk0** must be the drive where ProtectDrive is installed. Furthermore, ProtectDrive requires that the partition on **disk0** where the components will be installed is designated as drive letter **C:** within the operating system.

Multiple Boot System Preparation

If the system ProtectDrive will be installed on hosts multiple operating systems, it needs to be set up such that each partition can boot independently.

The setup of partitions needs to be complete before installing ProtectDrive on any of the partitions. Please refer to CHAPTER 20 for a detailed description of setting up a multiple boot system.

Installation Requirements

The following are the minimum requirements:

- IBM PC or 100 % compatible, with a Pentium CPU
- Memory - At least 32 MB system memory
- CD ROM Drive
or
access to a server-based installation directory (network installation)
- Hard Disk Space: ProtectDrive Setup Program requires 10 megabytes of free disk space on drive C. On exit, Setup will free most of this space and ProtectDrive will then take up only 4 Megabytes
- Operating System:
 - Microsoft Windows NT Workstation SP6a and Internet Explorer Version 4 or higher
 - Microsoft Windows 2000 Professional Edition with Service Pack 2 or greater
 - Microsoft Windows XP Professional Build 2600 Activated
- Token or smart card run time environment:
If users authenticate using tokens, the corresponding run time environment (RTE) needs to be installed. Please refer to CHAPTER 19 for details on supported tokens and installing their RTE.

Before Installation

Due to the complex nature of providing transparent disk encryption, ProtectDrive is not always compatible with existing software applications or processes. The following steps should be taken before installing ProtectDrive on a PC.

- Verify the integrity of the installation package.
All files in the installation package are electronically signed and the signatures are contained in a **.sig** file contained in the root folder of the CD-ROM or electronic archive.
Download the signature verification utility from the Eracom Web site and follow the instructions provided in the "FileVerify Technical Bulletin".
- Read CHAPTER 4 Considerations and Restrictions and CHAPTER 5 Incompatibilities, which detail compatibility considerations of the ProtectDrive system and any special conditions which may apply to your particular situation.
- From the **Start/Run** menu option, run **CHKDSK /f** on the C drive and all drives you wish to encrypt. This will check that the file system is intact and correct any errors.
- Backup all important data on the fixed disk(s) of your PC.
Installing ProtectDrive involves altering the contents of the fixed disk(s), so that, without ProtectDrive, the information is inaccessible. While this process has been made as safe as possible, a disk or power failure during the critical phases of the installation could result in loss of data.
- If you do not wish to allow addition of removable drives, ensure the maximum number of removable disk drives you wish to use with ProtectDrive are installed throughout the installation procedure. These drives can then be removed after installation, if desired.
- Ensure that you have at least 10 MB of free space available on your C drive.
- Ensure that a Windows installation has allocated the label C: to the system partition.

Choosing the installing user account

The user account that is used to install ProtectDrive is automatically added to the ProtectDrive user database, and the type of account and login method will determine a number of configuration options:

- The installing user must have administrative privilege on the computer being installed.
- If the account is a local account, the "Allow Local User Access" option will be enabled and cannot be disabled.
- If the account is a domain account and the user authenticates with their username and password, the "Allow Password Domain User Access" option will be enabled and cannot be disabled.
- If the account is a domain account and the user authenticates with their smart card and PIN, the "Allow Token Domain User Access" option will be enabled and cannot be disabled.

The installing user automatically becomes the ProtectDrive built-in Administrator - an account that cannot be removed. It is recommended that, if installing using a local administrative account, the Windows standard "Administrator" account is used to merge the roles of Windows and ProtectDrive administrator.

To utilize the selection of token groups or users that are granted access to ProtectDrive secured machines at installation time, the computer being installed must be a member of the relevant Windows domain and the installing user must log on to their domain account.

Note:

To avoid confusion as to which user is logged on during ProtectDrive installation, Windows should be configured to require the user to enter user name and password to log on to Windows.

This behavior is controlled in

- Windows 2000 by the "Users must enter a user name and password to use this computer" check box in the "Users and Passwords" tool in Control Panel/User Accounts.
- In Windows XP by the "Requires user to press Ctrl+Alt+Del" check box on the "Advanced" tab of the Control Panel/ User Accounts Applet.

Registration disk and recovery disk

A number of ProtectDrive files need to be stored on removable media and need to be presented at certain times during installation, decryption, and when using the ProtectDrive recovery tools.

All media containing the file Syskey.bin need to be stored securely since it is possible to access or decrypt protected systems if in possession of this file.

Registration disk

You can use an existing floppy diskette that contains your registration details and a recovery key issued by Eracom. The diskette contains the following files:

- Registration.txt
- Syskey.bin

Should this diskette be misplaced or damaged, Eracom will be able to produce a replacement disk if the registration serial number is known.

Starting with ProtectDrive 7.2.4 the registration process does not require registering the product with Eracom. Starting with ProtectDrive 7.2.4 Eracom does not issue registration files any more.

Administrators have the choice to install ProtectDrive with their existing registration files (syskey.bin and registration.txt) or to generate a new set of files.

The necessary keys and registration files are generated automatically during installation. It is recommended that this process is executed once; the generated files are securely backed up and are used in subsequent installations of the product.

Note: Eracom will not be able to recreate these files and it is the administrator's responsibility to ensure that the registration files are backed up and securely stored.

Note: The file syskey.bin contains the System Key and Recovery Key. This file needs to be kept physically safe, as possession of these files can ultimately provide access to protected systems and encrypted data.

The registration disk is required to:

- Install ProtectDrive
- Uninstall ProtectDrive
- Prepare a network installation of ProtectDrive

Recovery disk

Eracom recommends creating a recovery disk that contains the ProtectDrive recovery tools and the recovery keys (contained in the file Syskey.bin).

To create a recovery disk:

- Copy the files Registration.txt and Syskey.bin to a floppy disk.
- Copy the ProtectDrive recovery tools from the "Recovery" directory in the ProtectDrive distribution to this floppy disk.

The recovery disk is required to:

- Execute the ProtectDrive recovery tools
- Exercise user key recovery or new user introduction in the ProtectDrive Remote Recovery Administration console.

Note:

The recovery tools are 16-bit programs and require you to boot the system to be recovered to DOS. The recovery files can be on removable media other than floppy disk, but you must ensure that these files and programs are accessible from DOS.

Creating your own recovery keys

If you want to create your own recovery keys (i.e., not use the keys provided by Eracom), you can create your own from the ProtectDrive AutoRun menu.

- It is prudent to create a copy of your registration disk
- Select "Generate Recovery Keys" from the AutoRun menu
- Present the copy of the registration disk when prompted for the registration files.
- A new set of recovery keys will be generated and the registration details will be updated. The serial number associated with your copy of ProtectDrive will be retained.

Use this copy of the registration disk to perform ProtectDrive installation and prepare a recovery disk as described above.

Note:

If this procedure is used, Eracom will NOT be able to produce replacement registration disks and will not be able to recover any damaged, unbootable systems.

Phase 1. Starting the Installation Process

Note:

ProtectDrive can only be installed on the C drive. Installation attempts on drives other than C are detected and will not proceed.

- Close all Windows applications before starting the installation process.
- If installing from a CD-ROM, place the CD-ROM in the drive. After a few seconds the CD-ROM will auto run. If auto run has been disabled, open the disk and click on the autorun.exe file.
- If installing from an electronic archive (.zip file), extract all files into a folder of your choice, navigate to this folder, and click on the autorun.exe file.
- The AutoRun menu provides options to
 - Install or uninstall ProtectDrive.
 - Review the User Manuals and README.TXT file.
 - Prepare a Network Installation
(Network installation is described in the ProtectDrive Network Installation Guide, which can be found on the ProtectDrive CD-ROM)
 - Generate Recovery Keys
- After selecting the Install/ Uninstall option, the Installer will start.
- The Welcome Screen will be the first window to be displayed. Select [Next] to continue.
- The Eracom Software license agreement will be displayed. Select [Yes] if you accept the agreement.
- Select whether existing registration files will be used or a new set of files will be generated. Select [Next] to continue.
 - If the option to use existing files was selected, a valid set of registration files will be required before continuing. A folder browse dialog will be displayed for locating the files.
 - If the option to generate a new set was selected, select the location where the registration files should be stored. The files need to be present in the same location. We recommend storing the files on removable media, such as a USB memory stick or floppy disk. For disaster recovery purposes, a recovery floppy disk should be created as described above.

- After selection of the location, the necessary keys will be generated. A dialog is displayed that shows the progress of entropy collection for key generation. Moving the mouse cursor will accelerate this process. After the progress bar changes its colour to green, select [OK] to generate the keys.
- The following screen will ask for confirmation that the setup program has correctly determined which action to take:
 - Pre-Installation of ProtectDrive
 - Removal of an existing ProtectDrive installation
 - Upgrade of an existing ProtectDrive installation

Select [Next] if it is correct or select [Cancel] to abort the installation.

- The Setup Program will now install components necessary for the second phase of installation.
- The ProtectDrive Setup Program will be added to the Windows Start-up folder so the second phase of the installation will be started automatically the next time the PC is booted.
- By default, the setup program will reboot your PC at the end of this first phase of installation. Select [Finish] to complete pre-installation.
- After the reboot, the ProtectDrive setup program will automatically start to complete installation.

Phase 2. Completing the Installation

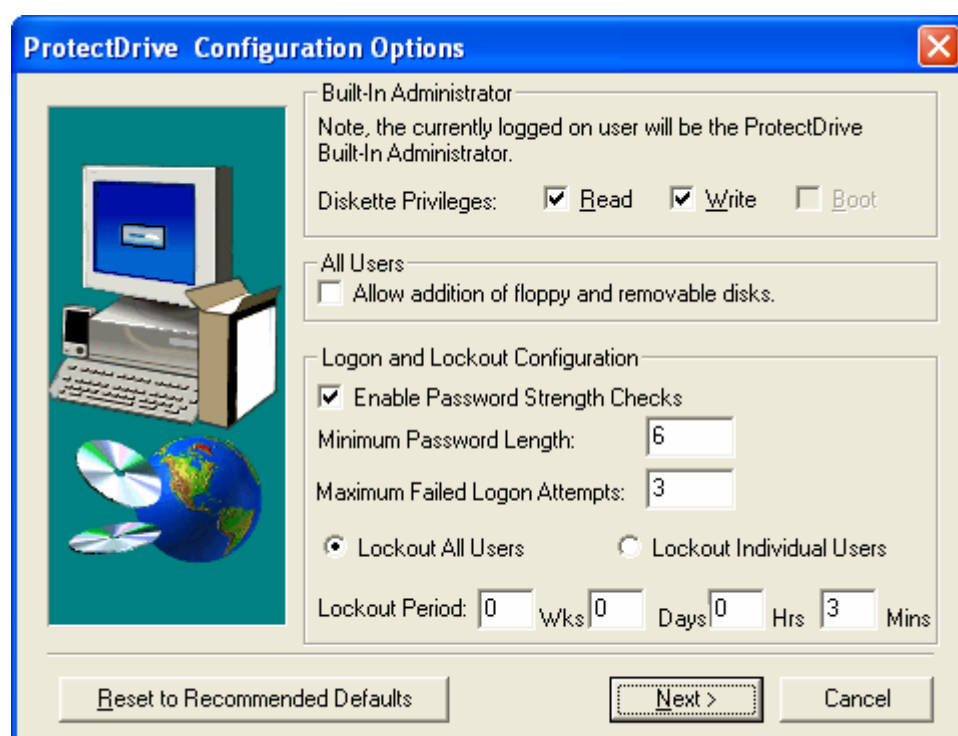
After logging on to Windows, the Welcome screen will again be displayed. The following will occur during this phase of installation:

- The set of registration files presented during pre-installation will be verified before continuing. A folder browse dialog will be displayed to locate the registration files.
- The next screen requires confirmation to complete installation. Select [Next] to continue.

- You will then be requested to select a Program Folder, which will contain the shortcuts to ProtectDrive applications. This folder will be accessible from the Start/Program menu on the Task Bar. “ProtectDrive” is the default selection. This is not the directory name under which files will be installed. Most ProtectDrive files are stored in the C:\SECURDSK directory. Select [Next] to continue.

Configuration Options

The next dialog allows the user to cancel the installation if they wish to change their ProtectDrive Built-in Administrator selection by logging on as another user. By default, the currently logged on user will be used as the ProtectDrive Built-in Administrator.



Diskette Privileges

Define the level of access the ProtectDrive built-in Administrator has to floppy diskettes. By default the built-in Administrator has maximum access to floppy disks.

Allow Addition of Floppy and Removable Disks

The default setting does not allow the addition of floppy and removable disks. See CHAPTER 4 for details on the implications of this setting. Internal ZIP drives are treated as another IDE drive not as an external ZIP drive.

Enable Password Strength Checks

If disabled, ProtectDrive will not check the strength of user passwords. Passwords are normally checked when a user is created, or their password is changed. This option should only be disabled if a corresponding Windows password policy is configured.

Minimum Password Length

The minimum password length that is required when a user enters a new password can also be set from this dialog (default=6). Setup will verify that the password length (of the current user) is at least this configured minimum.

Maximum Failed Logon Attempts

ProtectDrive will lock a computer after the specified number of unsuccessful logon attempts at the pre-boot logon screen have occurred. The default value is three (3).

Lockout All Users/ Individual Users

This setting determines whether access to all or individual user accounts is blocked for a period of time after too many failed logon attempts. The default is to lock out all user accounts.

Lockout Period

This value determines how long access to the system or an individual account is blocked. The default setting is three (3) minutes.

A system that is locked can be unlocked by exercising a recovery challenge/response mechanism.

Types of Users

ProtectDrive allows two types of users: Administrators and End Users. Within this User Manual, all non-administrative accounts will be referred to as End Users. All administrative accounts will be referred to as Administrators. All administrative and non-administrative accounts will collectively be referred to as Users.

Each ProtectDrive User (including Administrators) is classified as either a:

- Domain User,
- Local User or
- Token User

Additionally Administrator accounts are classified as:

- Built-in Administrator
- Windows Administrator.

Descriptions of the different Administrator and End User accounts are provided below:

Domain User

A Domain User is a user account that is used to log on to a Windows Domain. This type of authentication is used in a networked environment. For further information, see the documentation provided by Microsoft for your operating system.

Local User

A Local User is a user account that is used to log on to a computer with a Windows operating system installed. This type of authentication is used in a stand-alone environment. For further information, see the documentation provided by Microsoft for your operating system.

Token User

A Token User is a user account that uses a token and PIN combination as part of the authentication process. This type of authentication can only be used in a networked environment.

Built-In Administrator

A built-in Administrator is an administrative user account that is created at installation. This account type will be assigned to the user account used during the installation process of ProtectDrive. The user installing the product needs to be a Windows Administrator.

Windows Administrator

A Windows Administrator is an administrative user account that is created within the Windows operating system. A Windows Administrator is automatically assigned ProtectDrive Administrator privileges. This account is managed through the Windows operating system.

Authentication Settings

ProtectDrive can be configured to restrict access to various types of users:

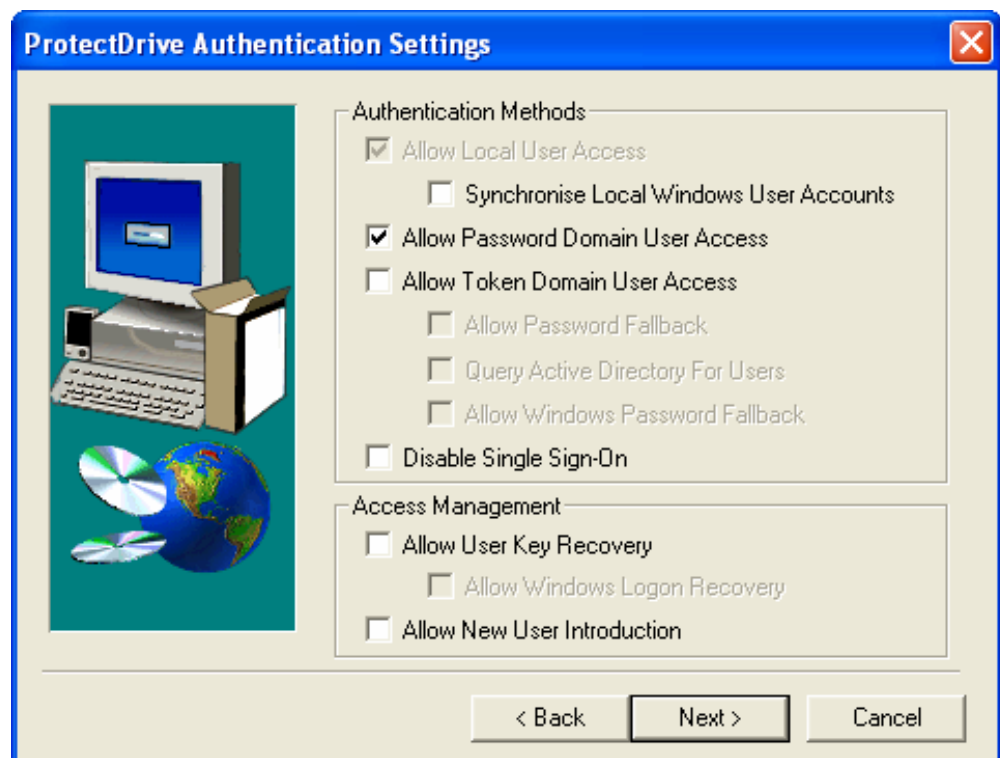
- Local Users;
- Password access by Domain Users;
- Token access by Domain Users;

In addition, special remote fallback and recovery options can be enabled:

- Password Fallback for Token Users;
- Password Recovery; and
- New User Introduction;

By default, Local Users and Domain Users are allowed and token access is not, unless the installing user has logged on to Windows with a token. Remote password recovery and new user introduction is disabled by default.

These options can be modified after installation by using the Advanced Configuration utility.



Note: It is not possible to disable the authentication method of the currently logged on user (The corresponding check boxes are grayed out).

Allow Local User Access

If this option is enabled, Local Users will be allowed to logon to the system. By default this option is enabled.

Synchronize Local Windows User Accounts

If Local User access is allowed, then this option may be configured. By default, it is enabled when Local User access is enabled.

If this option is enabled, existing local Windows usernames will be checked for compatibility with ProtectDrive and added to the ProtectDrive user database. The password of these users will be set to the default password, which can be configured during installation (see "One-Time Pre-Boot Password" below) and their Windows account is disabled.

If the "Synchronize Local Windows User Accounts" option is disabled, the user installing the product is the only user able to authenticate at pre-boot time.

Allow Password Domain User Access

If this option is enabled, Domain Users will be allowed to logon to the system using their username, domain name, and password. By default, this option is enabled.

Allow Token Domain User Access

If this option is enabled, Domain Users will be allowed to logon to the system using their logon token and PIN. The token must be a valid Windows logon token. ProtectDrive utilizes the user's X.509 certificate and RSA key pair to locate the user's account and decrypt the disk key.

Allow Password Fallback

If enabled, the user will be able to invoke the Password Fallback mechanism to retrieve a one-off password from an Administrator to gain access to the system from the pre-boot logon. See CHAPTER 10 for more details on this option.

Query Active Directory For Users

If selected, the installer will query Active Directory of the PC's domain and display a list of users and groups. A token account will be setup for the selected users, and users contained in the selected groups. It is only possible to query Active Directory if the current user is logged onto the domain.

Allow Windows Password Fallback

If this option is enabled and a token user logs on at pre-boot but the logon fails at Windows, ProtectDrive will allow the user to logon using a password. If necessary, this will bypass logon restrictions imposed by having "Allow Local User Access" or "Allow Password Domain Access" disabled. In addition, this option will force Single Sign-On from pre-boot to Windows. This feature is disabled by default.

Disable Single Sign-On

If this option is enabled, the system will not automatically logon to Windows after a pre-boot authentication. This feature is disabled by default.

Allow User Key Recovery

This allows the recovery of forgotten passwords to a computer without requiring the presence of an Administrator. This feature is disabled by default.

Allow Windows Logon Recovery

This option allows a user to automatically log on to their Windows account after exercising User Key Recovery. If enabled, the password recovery feature will store the encrypted user passwords in its user database. While the encryption is strong, this could be considered a security risk in certain environments.

Allow New User Introduction

This option is only available for password users (i.e., Local Users and Password Domain Users). If enabled, the user will be able to invoke the New User Introduction mechanism to retrieve a one-off access code from an Administrator to gain access to the system from the pre-boot logon. See CHAPTER 10 for more details on this option.

Select [Next] after the authentication settings are as required.

Certificate Selection

This configuration dialog is only shown if "Allow Token Domain Users" in the previous dialog was selected. It enables the administrator to control which certificates are able to be used for pre-boot authentication.

By default only the Microsoft Windows Smart Card Logon certificates will be used for pre-boot authentication.

Enhanced Key Usage

These settings define the Object Identifiers (OIDs) in the “Enhanced Key Usage” attribute of an X.509 certificate that need to be present for ProtectDrive to include the certificate in its user database.

If the “Smart Card Logon” check box is selected, certificates that include Smart Card Logon (1.3.6.1.4.1.311.20.2.2) in the “Enhanced Key Usage” field will be accepted by ProtectDrive.

If the “EFS” check box is selected, certificates that include Encrypting File System (1.3.6.1.4.1.311.10.3.4) in the “Enhanced Key Usage” field will be accepted by ProtectDrive.

Two additional OIDs can be specified to accept certificates that have other usages defined.

ProtectDrive accepts certificates that have **any** of the defined key usages.

Key Usage

The “Key Usage” field of an X.509 certificate represents a bit mask that defines the intended usage of the key (pair) associated with the certificate. Normally, selection of acceptable certificates via the Enhanced Key Usage attribute should be sufficient. To further narrow the range of certificates for use with ProtectDrive, the Key Usage can be specified here.

Note: Single Sign-On to Windows is only possible, if the token used for pre-boot logon also contains a Windows Smart Card Logon certificate.

Note: ProtectDrive adds certificates on installation by querying Active Directory when users first log on to Windows with their token, or when the `pduserdb.exe` is run. The settings defined here apply to all of the above methods.

Choose the required algorithms and select [Next].

Domain Users and Groups

If the “Query Active Directory For Users” option was enabled in the “Authentication Settings” configuration dialog, Setup will attempt to connect to Active Directory to retrieve a list of valid users and groups.

Select the groups or users that are allowed to access the PC and they will be added to the ProtectDrive user database.

Note: The user installing ProtectDrive must be logged in to their domain account for this feature to be available.

One-Time Pre-Boot Password

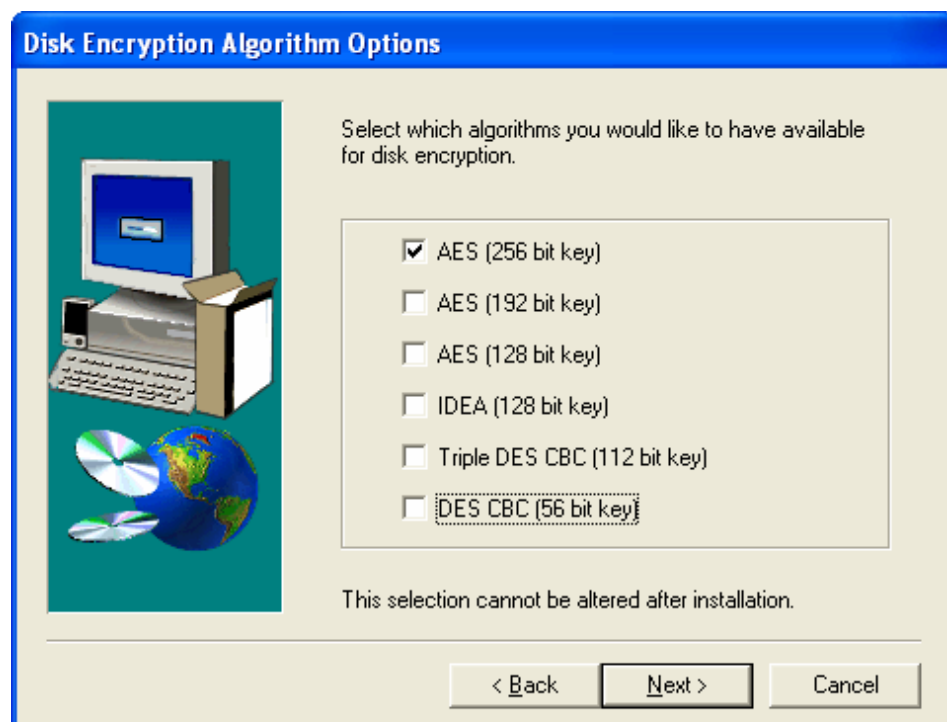
If “Synchronize Local Windows User Accounts” was checked, ProtectDrive will add all the local Windows users to its user database during installation and set their pre-boot password to this value. This one-time password will allow users to get through the pre-boot authentication, but logon to Windows will require users to enter their Windows password. After this initial Windows logon, the ProtectDrive pre-boot and Windows password will be synchronized.

Default Disk/Port Permissions

These permissions will apply to every user added to the ProtectDrive user database until they are updated via User Manager for local users, or the ProtectDrive Active Directory snap-in for domain users.

Disk Encryption Algorithm Options

The installer must select which disk encryption algorithms are required.



Choose the required algorithms and select [Next].

Multi-Boot Manager

If ProtectDrive detects more than one possible bootable primary partition, you will be prompted to enter user-friendly strings to identify these partitions. These strings will be displayed by the Boot Manager menu, which runs before the ProtectDrive pre-boot logon component and lets the user boot to different partitions. The default strings displayed during installation reflect the type of partition that has been located.

Installation Progress

ProtectDrive components and applications will be installed. Depending on the speed of your system, this stage of the installation can take some time, normally 3 to 5 minutes. A progress indicator will be displayed showing the percentage completed.

Note: It is important that this procedure is not interrupted as information on your fixed disk may be lost or the system rendered unbootable.

If the “Synchronize Local Windows User Accounts” option is enabled, existing local Windows user names will be checked for compatibility with ProtectDrive. If any are found to be incompatible, a window will be displayed listing the incompatible usernames and you will need to run the Windows User Manager from the [User Manager] button displayed on the window and correct the usernames. Only when all usernames are found to be compatible will you be able to continue.

To complete the installation the PC needs to be re-booted. Select [Finish] to complete the installation and re-start the computer. ProtectDrive pre-boot authentication is now active.

Note: The PC is only fully secured after all disks are **fully encrypted**. After verifying that the installation was successful and logging on to Windows, a warning message will be displayed as long as not all disks are fully encrypted. To start disk encryption, select [Encrypt Now] on the warning dialog.

Note: Some laptops have interchangeable CD and FD carriers. To install ProtectDrive, first insert the CD carrier and copy all the files to a directory on a hard drive. Then install the FD carrier (A: drive) and run **SETUP.EXE**

Installation of Server Components

- ProtectDrive supports central management of user port and disk access rights through an Active Directory server extension and a Microsoft Management Console snap-in. This provides an extra ProtectDrive tab in the server-side user management tool.

-

To install the server components:

- Log on to the schema master domain controller (schema FSMO role owner) as a user with privileges to extend the Active Directory schema.
- Execute the `server_setup.bat` file in the "Server " folder on the ProtectDrive CD-ROM.
- For each other domain controller, log on as a Domain Administrator and execute the `server_setup.bat` file.

Note: This will not affect the schema as it has been already modified in the previous step, but it will install the Microsoft Management Console snap-in.

Note: For details of Active Directory administration refer to the relevant Microsoft publications (e.g., the Windows Help information in Windows 2000 Server).

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 7

Single Sign-On Management

ProtectDrive may be used where a single sign-on user authentication system is in place or is to be deployed.

In a Windows only, single sign-on user authentication environment ProtectDrive will operate seamlessly without any setup being required.

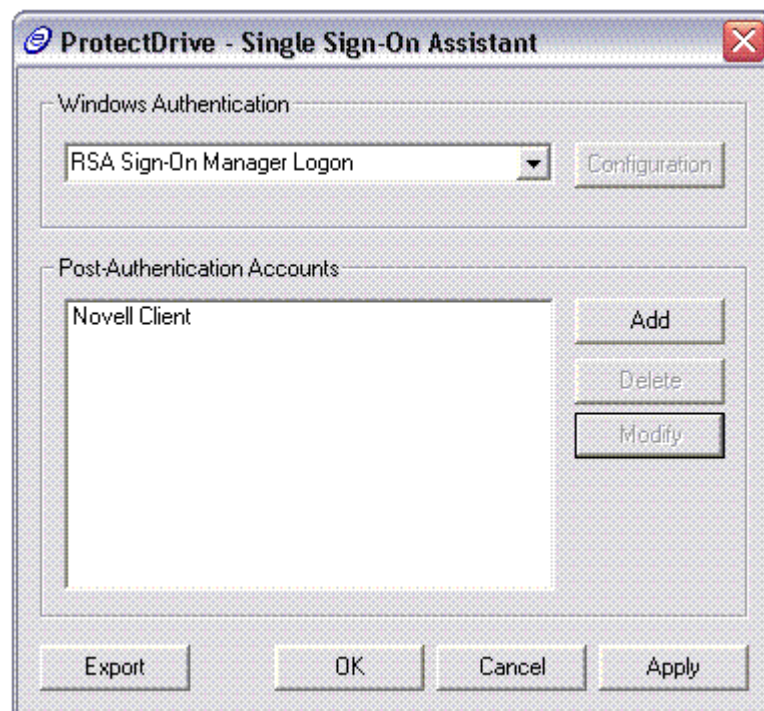
This chapter details the configuration of ProtectDrive for seamless operation in a single sign-on user authentication system environment where systems other than Windows are involved.

The Single Sign-On Assistant

Overview

The Single Sign-On Assistant is an application that manages all aspects of single sign-on for ProtectDrive. It is a flexible solution that enables users to configure the logon to their machine and other network services.

There are two components that Single Sign-On Assistant manages—Windows authentication accounts and post-authentication accounts. These are discussed in the following sections.



Accessing the Single Sign-On Assistant

To access the Single Sign-On Assistant, execute the file `ssoassistant.exe`. This file is located on the ProtectDrive installation CD in the *Recovery* folder.

Windows Authentication

Windows authentication allows users to select the GINA they would like ProtectDrive to work with. Currently, the choices are Standard Windows Logon (`msgina.dll`), RSA Sign-On Manager Logon (`3-gina.dll`), and Third Party Logon. Support for the Windows and RSA SOM GINAs is provided with ProtectDrive (see the section “RSA SOM Support” below), whereas a third-party logon must be configured by the user.

Configuration of third-party GINAs allows selection of the GINA DLL and manual entry of the dialog and control IDs for the GINA. These settings are stored in the registry for `pcvgina.dll` to access during Windows startup.

Post-Authentication Accounts

Post-Authentication accounts are provided to allow users to logon to multiple accounts that provide network services. Typically, this would be used to provide support for Novell networks (see the Novell Client Support section below), but there will be other specific user configurations which can benefit from using post-authentication accounts (see the “Third-Party Product Support” section below).

Each account can have an unlimited number of fields. Each field is configured by specifying which control in the application dialog box to fill with the required information (username, password, or domain). The pre-boot user's account details are used to perform the logon, so the username, password, and domain name must be the same.

A command is added to each account to logon to the account. It is selected by choosing which button on the application dialog box should be clicked to perform the logon action.

RSA SOM Support

Overview

RSA Sign-On Manager (SOM) is an application that performs single sign-on across a number of enterprise applications. It is advantageous that ProtectDrive collaborates with RSA SOM. This section discusses how this can be achieved.

Implementation

RSA SOM is supported in ProtectDrive by allowing the ProtectDrive GINA (pcvgina.dll) to chain the RSA SOM GINA. This allows the RSA SOM to function correctly, while providing single sign-on for pre-boot users.

The ProtectDrive GINA loads the RSA SOM GINA dialog configuration when the Chained GINA registry value is set to the RSA SOM GINA. This can be configured by using the ProtectDrive Single Sign-On Assistant.

Considerations

Currently, the Single Sign-On Assistant and ProtectDrive GINA assume that the RSA SOM GINA is located in the standard location (C:\Program Files\RSA Security\RSA Sign-On Manager Client\3-Gina.dll). If this is not the case, third-party GINA support should be used in the Single Sign-On Assistant, with the dialog configuration as follows:

- Notice Dialog: ID = 100
- Logon Dialog: ID = 113, Username ID = 1000, Password ID = 1008, Domain ID = 1009
- Change Password Dialog: ID = 800
- Ctrl + Alt + Del Dialog: ID = 400
- Locked Dialog: ID = 200
- Unlocked Dialog: ID = 106, Username ID = 1000, Password ID = 1002, Domain ID = 1009
- Shutdown Dialog: ID = 500

Third-Party Product Support

Overview

There are a number of third-party products that are often used concurrently with ProtectDrive. It can be beneficial if ProtectDrive can perform single sign-on for these products, while not requiring the direct support for each product. This section discusses how this can be achieved in a flexible and minimal manner with ProtectDrive using the Single Sign-On Assistant.

Support for Third-Party GINAs

ProtectDrive GINA supports the chaining of any third-party GINA. In this case, the dialog configuration for the chained GINA is set up using the Single Sign-On Assistant, and is stored in the registry. ProtectDrive GINA loads this configuration at start up and performs single sign-on.

It is not guaranteed that this approach will work for every third-party GINA, as there is considerable flexibility with the implementation of replacement GINAs. Instead, single sign-on for GINAs which "play fair" is offered.

At this stage, the user must manually enter the dialog and control IDs using Single Sign-On Assistant. The user must be able to source this information from the seller/manufacture of the third-party product. Dynamic discovery, as used for post-authentication accounts, may be added in future releases.

Support for Third-Party Accounts

Logging on to third-party products can occur using a post-authentication approach. In this case, ProtectDrive GINA and the chained GINA are used to log on to Windows. Then each third-party product is logged on to when the Windows shell is initialized.

This is only possible if the third-party product provides a logon application. Then the Single Sign-On Assistant can be used to create a post-authentication account which can be run to log on to the product using the logon application.

Novell Client Support

Overview

This section discusses ProtectDrive support for single sign-on when using Novell clients.

Implementation

The approach taken when using ProtectDrive is to logon to Novell services post-authentication using the Novell logon application.

A post-authentication account for the Novell logon application can be created using the Single Sign-On Assistant. In this process, the Single Sign-On Assistant discovers the username, password, and domain fields, and the logon command. This information is then used to automatically logon to Novell during shell startup.

Known Issue

For password synchronization to work, the Novell GINA logon must be used, not the post-authentication logon.

Administrative Procedures**Configuration after ProtectDrive Installation Over an Existing System**

1. User installs the ProtectDrive package on the system.
2. Installation completes normally.
3. Either:
 - User runs the Single Sign-On Assistant to configure the SSO settings.
 - User imports SSO configuration by running the registry file (*.reg) exported from the Single Sign-On Assistant.

Configuration after Installing Additional Software to the ProtectDrive System

1. User installs additional software to the ProtectDrive system that installs a replacement GINA.
2. User runs the Single Sign-On Assistant, which detects the new replacement GINA and asks if they would like to chain the replacement GINA with the ProtectDrive GINA.
3. Either:
 - User selects not to chain the GINA and is warned of the security implications of their selection. ProtectDrive can't provide single sign-on and cannot enforce the login method.
 - User selects to chain the replacement GINA, so the Single Sign-On Assistant chains the GINA and the user can set the GINA configuration.

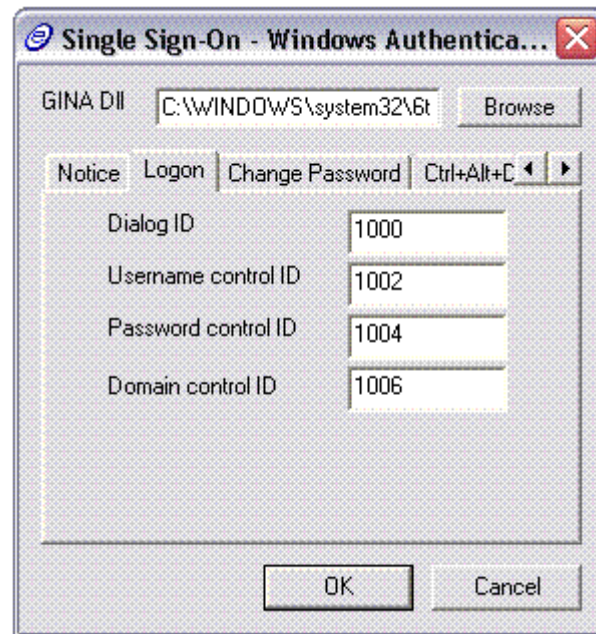
Note: The user must run the Single Sign-On Assistant after the installation of any additional software.

Changing Chained GINA

1. User runs the Single Sign-On Assistant.
2. User selects desired GINA in the Single Sign-On Assistant.
3. If a third-party GINA, the Single Sign-On Assistant must be used to specify the GINA configuration.
4. Either:
 - User selects OK or Apply and the Single Sign-On Assistant commits the GINA selection.
 - User selects Cancel and the new GINA selection is thrown away.
5. The Single Sign-On Assistant exits.

Setting GINA Configuration

1. User runs the Single Sign-On Assistant.
2. User selects a third-party GINA (Standard Windows and RSA SOM GINAs are automatically configured).
3. User opens the modal GINA configuration dialog by clicking the "Configuration" button.
4. User must select the GINA DLL filename and location.
5. For each GINA dialog of interest to the ProtectDrive GINA, the user specifies the dialog and control IDs for the third-party GINA (shown below). If any of the IDs are left unspecified, the user is warned that this can create unexpected behavior in the ProtectDrive GINA.

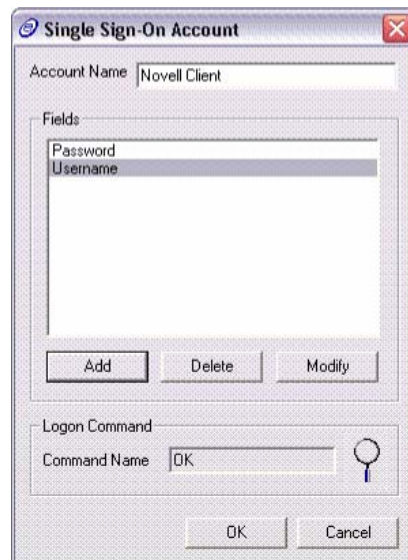


6. Either:
 - the user selects OK and the settings are stored (but not committed).
 - the user selects Cancel and the settings are thrown away.
7. GINA configuration dialog closes and the main Single Sign-On Assistant dialog box displays.
8. Either:
 - the user selects OK or Apply and the settings are committed.
 - the user selects Cancel and the settings are thrown away.
9. The Single Sign-On Assistant exits

Creating a Post-Authentication Account

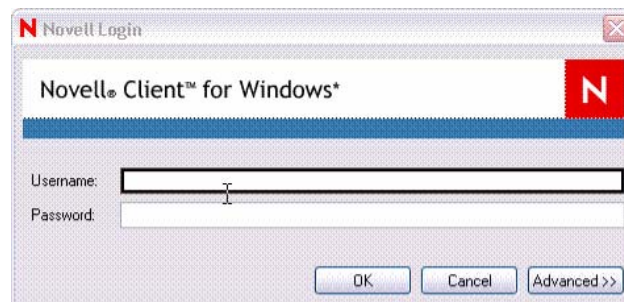
1. User runs the Single Sign-On Assistant.
2. User creates a new account by clicking on the "Add" button.

The *Single Sign-On Account* dialog box displays.

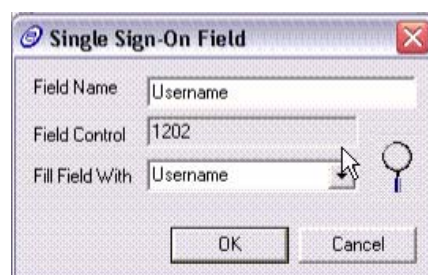


3. User can then specify a name for the account, which must be unique.
4. User runs the application which performs the post-authentication account logon.

For example:



5. User adds one or more fields by clicking on the "Add" button in the *Single Sign-On Account* dialog box. The *Single Sign-On* field dialog box displays.



6. User drags the magnifying glass icon/cursor from the *Single Sign-On* field dialog box to the field required on the application logon Window.

Field Name and *Field Control* details appear in the *Single Sign-On* field dialog box as shown in the screen shot above.

7. User makes the selection required in the *Fill Field With* field and clicks *OK*.
8. User selects the logon command (the button on the application which performs the logon) by dragging the magnifying glass icon/cursor from the *Single Sign-On Account* dialog box over the button on the application.
9. Either:
 - the user selects *OK* and the account is stored.
 - the user selects *Cancel* and the account is not created.
10. The Account dialog box closes and user is returned to the main Single Sign-On Assistant dialog box.
11. Either:
 - the user selects *OK* and the account is committed.
 - the user selects *Cancel* and the account is not created.
12. The Single Sign-On Assistant exits.

Modifying a Post-Authentication Account

1. User runs the Single Sign-On Assistant
2. User selects the account to modify from the accounts list and clicks on the "Modify" button.
3. The account dialog box appears with the account information.
4. The user changes the account information as required.
5. Either:
 - the user selects *OK* and the new account information is saved.
 - the user selects *Cancel* and the account information is thrown away.
6. The Account dialog box closes and the user returns to the Single Sign-On Assistant dialog box.
7. Either:
 - the user selects *OK* and the new account information is committed.
 - the user selects *Cancel* and the new account information is thrown away.
8. The Single Sign-On Assistant exits.

Removing a Post-Authentication Account

1. User runs the Single Sign-On Assistant.
2. User selects the account to remove from the accounts list and clicks on the "Delete" button.
3. Either:
 - the user selects OK and the account deletion is committed.
 - the user selects Cancel and the account is not deleted.
4. The Single Sign-On Assistant exits.

Creating a Post-Authentication Account Field

1. User runs the Single Sign-On Assistant.
2. User creates a new account by clicking on the "Add" button, or modifies an existing account by clicking on the "Modify" button.
3. The user runs the application which performs the post-authentication account logon.
4. The Accounts dialog box appears and the user clicks on the "Add" button.
5. The Field dialog box appears.
6. The user can specify a field name which is unique to the account.
7. The user must select the field control by dragging the "magnifying glass" icon/cursor over the control to be filled in the application.
8. User selects what information is used to fill the field.
9. Either:
 - the user selects OK and the field is stored in the account.
 - the user selects Cancel and the new field is thrown away.
10. Field dialog box closes and user returns to the account dialog box.
11. Either:
 - the user selects OK and the account is stored.
 - the user selects Cancel and the new account/information is thrown away.
12. Account dialog box closes and user returns to the Single Sign-On Assistant dialog box.

13. Either:
 - the user selects OK and the account is committed.
 - the user selects Cancel and the account is thrown away.
14. The Single Sign-On Assistant exits.

Modifying a Post-Authentication Account Field

1. User runs the Single Sign-On Assistant.
2. User modifies an existing account by clicking on the "Modify" button.
3. The user runs the application which performs the post-authentication account logon.
4. The Accounts dialog appears and the user clicks on the "Modify" button.
5. The Field dialog box appears.
6. User modifies the file information.
7. Either:
 - the user selects OK and the modified field is stored in the account.
 - the user selects Cancel and the new field information is thrown away.
8. The Field dialog box closes and user returns to the account dialog box.
9. Either:
 - the user selects OK and the account is stored.
 - the user selects Cancel and the new field information is thrown away.
10. The Account dialog closes and the user returns to the single sign-on assistant dialog box.
11. Either:
 - the user selects OK and the new field information is committed.
 - the user selects Cancel and the account is thrown away.
12. The Single Sign-On Assistant exits.

Removing a Post-Authentication Account Field

1. User runs the Single Sign-On Assistant.
2. User modifies an existing account by clicking on the "Modify" button.
3. The user runs the application which performs the post-authentication account logon.
4. The Accounts dialog box appears and the user clicks on the "Delete" button.
5. Either:
 - the user selects OK and the field is removed temporarily from the account.
 - the user selects Cancel and the field remains in the account.
6. The Account dialog box closes and user returns to the main the Single Sign-On Assistant dialog box.
7. Either:
 - the user selects OK and the field is permanently deleted from the account.
 - the user selects Cancel and the field remains in the account.
8. The Single Sign-On Assistant exits.

Exporting SSO Settings

1. User runs the Single Sign-On Assistant.
2. User clicks the "Export" button.
3. User selects the file to export the settings to.
4. The Single Sign-On Assistant reports successful export, and then exits.

CHAPTER 8

Upgrading ProtectDrive

The ProtectDrive installation program will automatically select to upgrade your current version of ProtectDrive if it is possible. If the currently installed version of ProtectDrive can be upgraded, there is no need to decrypt the hard drives.

The following versions of ProtectDrive can be upgraded to this version.

- ProtectDrive for Windows 2000/XP v6.0.0
- ProtectDrive for Windows 2000/XP v6.0.1
- ProtectDrive for Windows 2000/XP v6.0.2
- ProtectDrive for Windows 2000/XP v7.0.1
- ProtectDrive for Windows 2000/XP v7.0.2
- ProtectDrive for Windows 2000/XP v7.1.0
- ProtectDrive for Windows 2000/XP v7.1.1
- ProtectDrive for Windows v7.2.X, where $X \geq 0$

If your currently installed version of ProtectDrive is not listed above, you must uninstall the installed version of ProtectDrive, and then install this version of ProtectDrive.

Before updating, the ProtectDrive Upgrade Program will archive the current files and components of ProtectDrive. Should an error occur during the upgrade process, these archived files and components will be restored.

It is important that you re-start your PC when prompted at the end of an upgrade or restore.

Upgrading the Recovery Tools

To create a diskette containing the latest version of the ProtectDrive diagnostic and recovery tools, copy the files contained in the “Recovery” directory on the installation CD to a diskette. It is important that only the correct version of the recovery and diagnostic tools be used.

Upgrading

1. Close all open program and files, including the ProtectDrive disk encryption reminder.
2. Select Install/Upgrade from the AutoRun menu.

Note: Upgrades must only be run on non-faulty ProtectDrive systems. Upgrading does not repair ProtectDrive.

Network Upgrades

Similar to interactive or automatic network installations, upgrades can be performed from a central server location. The process of preparing such a network upgrade is the same as for installation.

Please refer to the Network Installation Guide, which is available on the ProtectDrive CD and can be accessed via the AutoRun menu, for details and proceed as prompted. During the upgrade process you will be prompted to edit the install/upgrade response file (install.rsp). Not all sections in this file will be processed during an upgrade.

Note: The Crypdisk response file will also be displayed for editing but will be ignored by the upgrade process.

If an automated network upgrade is performed UPDATE.LOG will be created in the directory selected during the preparation process.

Note: Ensure that the diagnostic and recovery tools are updated to match the version of ProtectDrive. The new recovery tools are in the “Recovery” directory on the installation CD or electronic archive (.zip).

It is VERY IMPORTANT that old versions of recovery tools not be used on upgraded systems, since these old versions might not be version-aware and can potentially corrupt the installation.

Upgrading a ProtectDrive version earlier than 7.2.2

Authentication Settings

The current ProtectDrive installation will have a populated user database. With the introduction of two-factor authentication, it is necessary to align the user database with the authentication settings specified during the upgrade. For example, if after the upgrade, users can only log on with their Windows logon token, their username and password access must be removed.

ProtectDrive upgrade will add and delete users from the current user database depending on the authentication settings. The user performing the upgrade will always remain a valid ProtectDrive user. The update program guarantees this by preventing the installer from disabling the authentication method used to log on to Windows.

Thus, to create a token-only system, the installer needs to log on to Windows with their token to be able to disallow password authentication at pre-boot time.

During an upgrade, the authentication settings are configured via the same dialog as at installation. Refer to CHAPTER 6, Authentication Settings, for details on these settings.

Default Disk/Port Permissions

These permissions will apply to every user added to the ProtectDrive user database until they are updated via User Manager, for Local Users, or the ProtectDrive Active Directory snap-in for domain users.

Upgrading from PCVault 5.12.4

It is not possible to directly upgrade to this version of ProtectDrive. Installations of ProtectDrive (PCVault) 5.12.4 either need to be removed or upgraded to ProtectDrive 7.2.3 prior to being upgraded to this latest version of ProtectDrive

Floppy Disk Configuration

To ensure that ProtectDrive will recognize your floppy disk drives, it is necessary, after upgrading, to log on as a Windows Administrator. This will update the ProtectDrive information for floppy disk drives. All floppy disk drives present at this time will be accessible after the next reboot.

If, for some reason, this fails, the utility can be run manually by opening a command prompt, executing the following command, and then rebooting.

```
rundll32c:\securdisk\binnt\update.dll,PCVUpdFloppyDTE
```

If, for some reason, an error occurred during the upgrade, and PCVault 5.12 is restored, the following error will be displayed the next time you log on:

Unable to locate c:\securdisk\binnt\update.dll

This is expected behavior, and the error message can be ignored.

Restoring ProtectDrive

Should it be necessary to restore your previous version of ProtectDrive following an upgrade, run SETUP.EXE from the C:\SECURDSK\BINNT\ARCHIVEvn_nn directory, where vn_nn is the version of ProtectDrive that was upgraded.

All files archived during the most recent upgrade will be restored.

Removing the Upgrade Archive

As soon as you are satisfied that it will not be necessary to restore from the backup it is good practice to delete the archive created by the Upgrade process.

Using Windows Explorer, delete the directory from the C:\SECURDSK\BINNT\ARCHIVEvn_nn directory, where vn_nn is the version of ProtectDrive that was upgraded.

CHAPTER 9

Uninstalling ProtectDrive

Normal Uninstall

Note: Before ProtectDrive can be removed, all disks must be fully decrypted.

- Launch the cryptdisk utility by clicking on “Encrypt-Decrypt HardDisks” in the Start/Programs menu.
- Fully decrypt all disks. (see CHAPTER 15 Encrypt-Decrypt Hard Drives for details)
- From the Control Panel, run the Add/Remove Programs applet.
- Select ProtectDrive, and then click on Add/Remove.
- The ProtectDrive Setup Program will take a few moments to load.
- Follow the on-screen prompts.
- The correct registration disk, used for installation, will be required prior to an starting the uninstallation.

In some cases, where ProtectDrive components have been corrupted or removed, uninstallation can still proceed. If Setup reports a problem and you are unable to uninstall, contact Eracom support.

Problems with Uninstall

If there is a problem with Windows, for example, if the user is forced to use Safe Mode, ProtectDrive has a fallback uninstall procedure. Use the ProtectDrive installation CD and run the program:

```
setup.exe /uninst
```

Note: Do not force the uninstallation on encrypted disks. Use the DECDISK utility on the diagnostic disk to fully decrypt all hard disks before running setup.exe with the /uninst switch.

See CHAPTER 14 - Recovery Tools for details on the DECDISK utility.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 10

Logging On

Pre-Boot Authentication

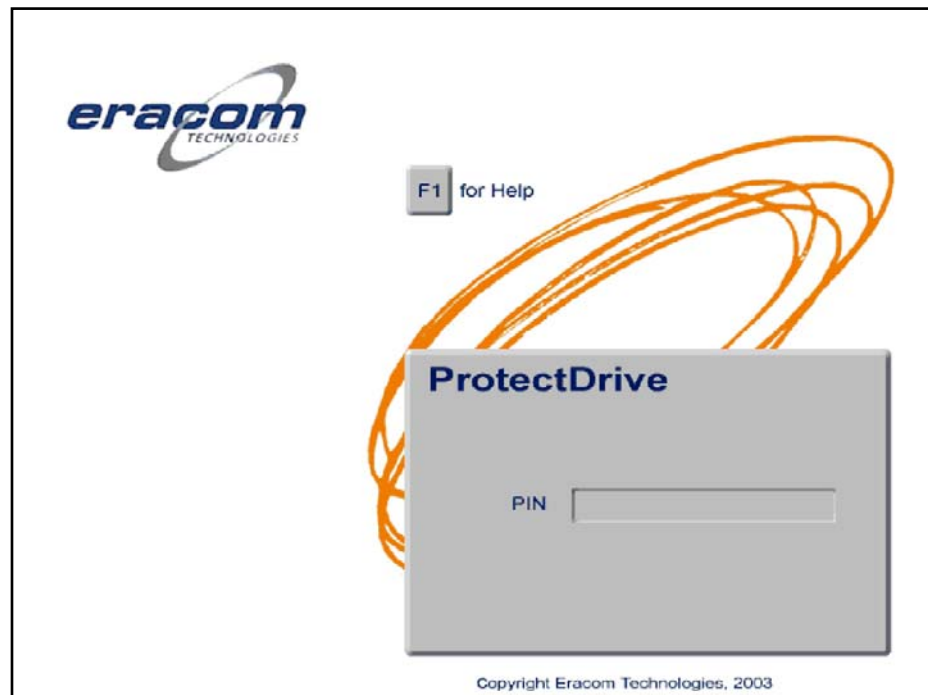
When the PC is turned on or rebooted, the ProtectDrive protection system will request the identity of the person requiring access. This is the process of System Logon. When initiated in this way, ProtectDrive will display a logon screen. The logon method is determined during installation.

Please refer to the Authentication Settings section in CHAPTER 6 for details on ProtectDrive installation and configuration of the logon system.

If token or smart card logon is enabled, the PIN entry screen is displayed after the PC is powered up. Otherwise, the username/password entry screen is displayed.

If both methods are allowed, the PIN entry screen is displayed by default and the user can switch between PIN entry and username/password entry screen by pressing the F2 key.

Token or Smart Card Logon



With the PIN entry mask displayed, insert your token or smart card and enter the PIN. ProtectDrive will verify the PIN and the user certificate stored on the token or smart card. If the verification is successful, the boot process will continue.

The authentication could fail for one of the following reasons:

- Token or smart card not inserted or faulty.
- Incorrect PIN.
ProtectDrive will allow a number of attempts to enter the correct PIN. After the maximum number of unsuccessful attempts is reached, the PC is locked. Refer to CHAPTER 6 for details on locking and unlocking configuration.
Tokens and smart cards can be configured to allow a maximum number of PIN validation attempts. After this number is reached, the token needs to be unlocked or re-initialized.
- Missing or invalid logon certificate.
Before tokens or smart cards can be used to log on to ProtectDrive, they need to be initialized and a valid Windows logon certificate needs to be stored on the token or smart card.

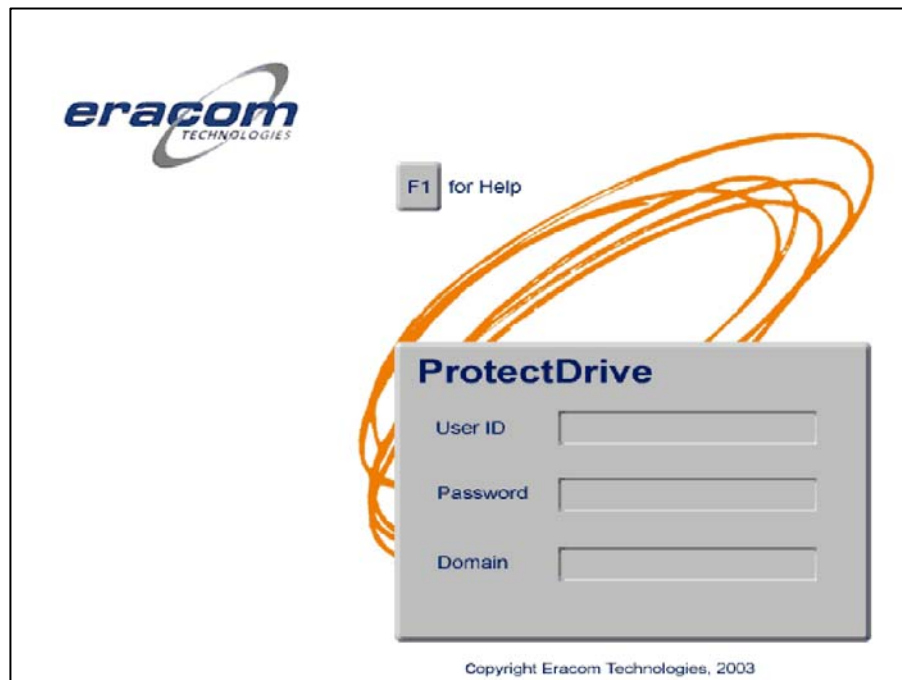
If one of these errors occurs (except in the case of incorrect insertion or faulty smart card or token), a corresponding error message is displayed and an invalid logon attempt is recorded in the audit log.

Please refer to CHAPTER 19 for details on preparing tokens for use with ProtectDrive.

Password Fallback

If enabled during installation or subsequently through the “Advanced Configuration” application, users who normally log on to the computer with their token can fall back to username and password authentication in case their token is lost. This option is similar to the “New User Introduction” feature described below and is meant for one-off, emergency access to a PC.

To invoke password fall back, the user must have the cursor in the PIN entry field and press Shift-F9.



Password Logon

If a correct combination of username, password and domain or local machine name is provided, ProtectDrive will proceed with the system start. If the combination is incorrect, ProtectDrive will request the logon process be retried.

Note: Select the domain by choosing the local machine name or the name of the desired Windows domain with the up and down arrow keys.

Windows Logon

Due to the single sign-on functionality of ProtectDrive, the normal Windows logon will not appear when restarting the machine unless the [Shift] key is held down during Windows startup.

Alternatively - to always show the Windows logon - Check the “Disable Single Sign-On” option in the Advanced Configuration Options program under the “Logon Control” tab.

First Time Logon

ProtectDrive will only allow users to log on to a machine at pre-boot if it recognizes them, i.e. ProtectDrive has the user's identification in its database. This database is synchronized with the Windows user database and if users are added to Windows via the Windows user management tool or log on to their domain account, they are also added to the ProtectDrive user database. Conversely, if a user is removed from the Windows user database, they will not be able to log on to ProtectDrive. Refer to CHAPTER 16 for details of user management.

New User Introduction by Existing Administrator

Thus, one method of introducing a new user to a computer secured by ProtectDrive is for an existing Administrator to log on to ProtectDrive and allow the new user to logon to Windows. ProtectDrive will add this user to its database and allow the user to log on in the pre-boot phase.

New User Introduction in the Absence of an Existing Administrator

If it is not practical to have an existing Administrator present the first time a new user logs on to a machine, users can be introduced by obtaining an access code from an Administrator, for example via telephone.

ProtectDrive provides a challenge/ response procedure that will provide a one-off access code that will allow new users through the pre-boot authentication phase. They will then have to log on to Windows and ProtectDrive will add the new user to its database.

To invoke the challenge/ response procedure, the user must have the cursor in the username entry field of the password logon and press Shift-F9.



Note: This function is only active if either the remote password recovery or password fallback feature is enabled. See CHAPTER 6 for details.

The user then identifies himself to an Administrator and communicates the serial number and recovery code to the Administrator.

The Administrator enters the details into the Remote Recovery Administration console and communicates the access code, displayed in the Response field of the console, to the user.

The user enters the response in the fields provided in the recovery screen and presses the Enter key. If the response was entered correctly, the user is logged on and the operating system boot process starts.

Note: Because the access code is randomly generated and comparatively long, it will be displayed on the screen to avoid unsuccessful logons. This is not a security risk since the access code can only be used once and will be re-generated the next time the challenge/ response procedure is invoked.

Unsuccessful Logon

ProtectDrive will allow a number attempts (three (3) by default) for users to correctly identify themselves. If a correct combination of username, password and domain name or token and PIN has not been input, ProtectDrive will lock the PC for a configurable period of time (three (3) minutes by default). During this period no further logon attempts will be permitted.

If after this period user identification fails again at the next attempt, ProtectDrive will lock the PC again for the configured period of time. ProtectDrive uses this system to inhibit out of hours password or PIN guessing attacks.

Successful Logon

Just before the Windows shell is started, a Logon Information Message will appear. The information shows the name of the user who logged on, the time they logged on, the time of the last password change (if applicable) including the number of logons since that change and the total number of logons.

An Administrator can turn off this message. Refer to Advanced Configuration Options in CHAPTER 11 for details.

Unsuccessful Logon Attempt Warnings

If there have been unsuccessful attempts to logon to the PC, the count(s) will be displayed in a warning message. These counts are reset when a successful logon is accomplished.

The unsuccessful logon warnings are designed to alert the user to the possibility of an attempted break-in to the PC.

This warning message can be turned off and an optional system defined message can be displayed. Refer to Advanced Configuration Options in CHAPTER 11 for details.

Diskette Boot

If a bootable floppy diskette is inserted into the A drive and the PC is reset, then the PC will boot from the diskette. ProtectDrive cannot stop this, however if the hard disk is encrypted there will be no meaningful data accessible on the hard disk.

Note: Unencrypted drives are fully accessible after booting from a floppy disk using this method. Therefore all disks with sensitive data should be encrypted after installation.

Any attempt to ‘fix’ the hard disk will result in corruption of the hard disk contents.

Refer to CHAPTER 16, Privileges and Access Permissions, for more information.

Token Removal

Computers using tokens or smart cards for Windows logon can be configured to automatically lock the workstation when the token or smart card is removed.

This behavior is controlled by the “Smart card removal behavior” policy in the Local Security Settings. By default, this policy is set to “No action” or “Not defined.”

Eracom recommends setting this policy to “Lock Workstation.” This setting will require the user to re-insert their token and enter their PIN upon return to the workstation.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 11

Configuring ProtectDrive

After Installation

After installation of the ProtectDrive software, it will be necessary to perform the following configuration steps.

- Logon to the system by entering ProtectDrive's built-in Administrator's username and password – these entries are case-sensitive so be sure to enter them correctly.
- If entered correctly, the system will then continue the boot process normally.

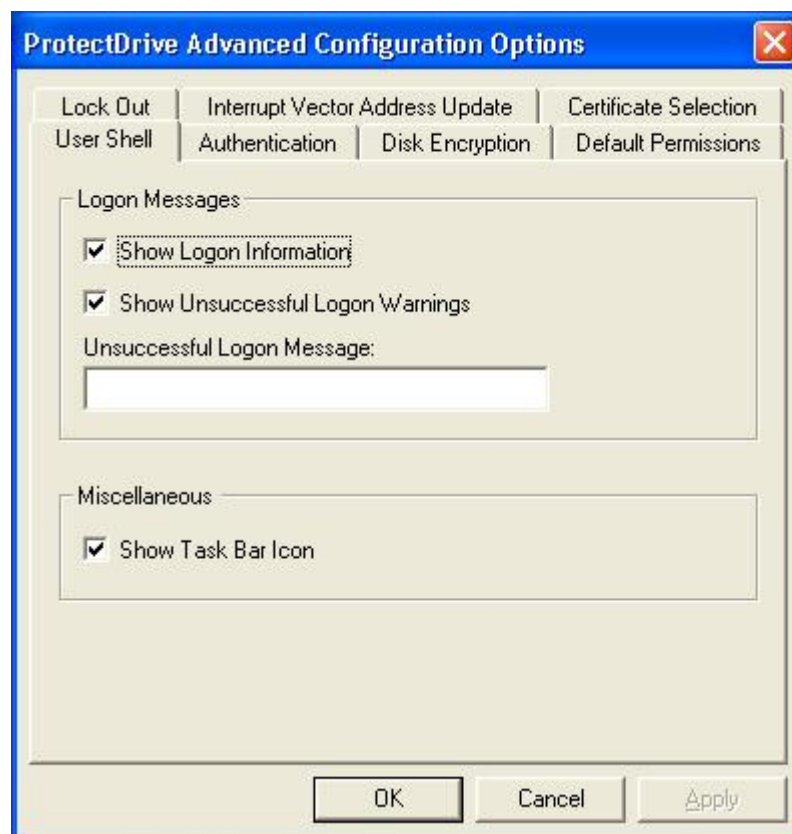
It is now advisable to:

- Fully encrypt all hard drives. Refer to CHAPTER 15 Encrypt-Decrypt Hard Drives for details. By default, after every logon, a reminder warning will be displayed if one or more drives are not fully encrypted.
- Read the section on User Management and use the Windows User Manager application to change any passwords for users added or modified during the installation.
- Store the built-in Administrator's name and password securely with the ProtectDrive registration and recovery disks.

Advanced Configuration Options

The Advanced Configuration program is invoked by clicking on the "Advanced Configuration" item in the Start/Program Files/ProtectDrive menu. The configuration options replicate the options available at installation time to enable system configuration post installation.

User ShellTab



Show Logon Information

By default, a logon information message is displayed once a user has successfully logged onto ProtectDrive. This message shows the date and time of the last successful logon, the date and time of the last password change, and the number of successful logons.

Uncheck this option to disable displaying of logon information.

Show Unsuccessful Logon Warnings

A warning message is displayed if previous unsuccessful logon attempts have occurred. The displaying of the unsuccessful logon warning message can be disabled by unchecking this option.

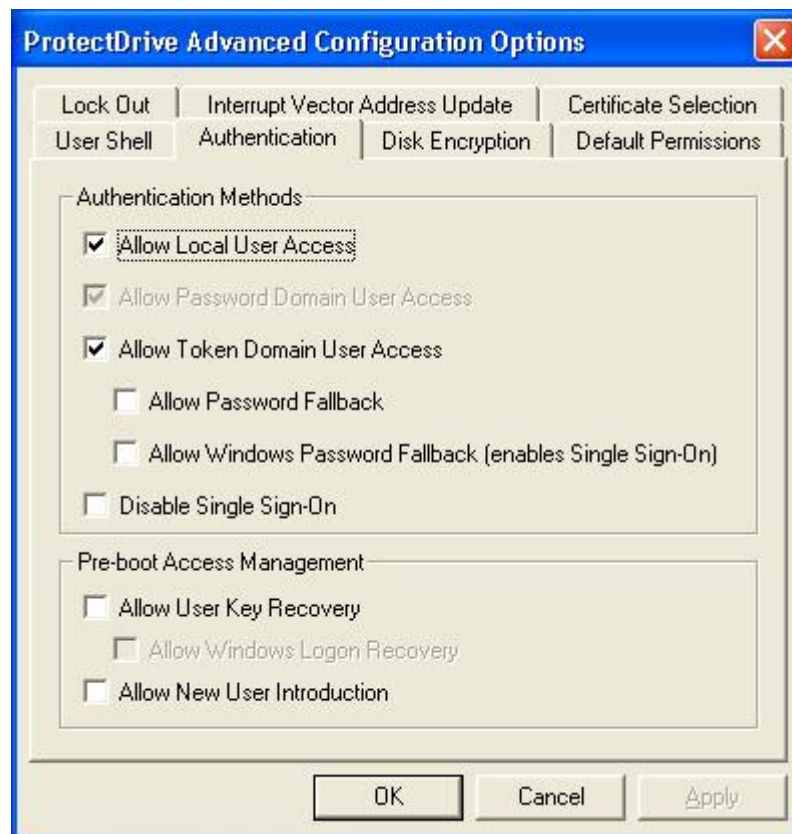
Unsuccessful Logon Message

When the "Show Unsuccessful Logon Warnings" option is checked, an optional message can also be displayed by entering this message in the "Unsuccessful Logon Message" field.

Show Task Bar Icon

By default, a small key symbol is shown in the task bar notification tray after ProtectDrive installation. Double-click on the icon to lock the system. This icon can be disabled by clearing this checkbox.

Authentication Tab



Allow Local User Access

If this option is enabled, Local Users will be allowed to logon to the system. By default, this option is enabled.

Note: It is not possible to remove the authentication method of the currently logged on user, nor is it possible, in unregistered installations, to remove the authentication method of the installer.

Allow Password Domain User Access

If this option is enabled, Domain Users will be allowed to logon to the system using their username, domain name, and password. By default, this option is enabled.

Allow Token Domain User Access

If this option is enabled, Domain Users will be allowed to logon to the system using their logon token and PIN. The token must be a valid Windows logon token. ProtectDrive utilises the user's X.509 certificate and RSA key pair to locate the user's account and decrypt the disk key.

Allow Password Fallback

This option is only available for Token User Access. If enabled, the Token User will be able to invoke the Password Fallback mechanism to retrieve a one-off password from an Administrator to gain access to the system from the pre-boot logon. See CHAPTER 10 for more details on this option.

Allow Windows Password Fallback

This option is only available for Token User access. If this option is enabled and a token user logs on at pre-boot but the logon fails at Windows, ProtectDrive will allow the user to logon using a password. If necessary, this will bypass logon restrictions imposed by having "Allow Local User Access" or "Allow Password Domain Access" disabled. In addition, this option will force Single Sign-On from pre-boot to Windows. This feature is disabled by default.

Disable Single Sign-On

Due to the single sign-on functionality of ProtectDrive, the normal Windows logon dialog will not appear when restarting the machine. To always show the Windows logon, this checkbox should be selected. This functionality also enables a new domain name to be entered or to logon as another user.

Allow User Key Recovery

This allows the recovery of forgotten passwords to a computer without requiring the presence of an Administrator. This feature is disabled by default.

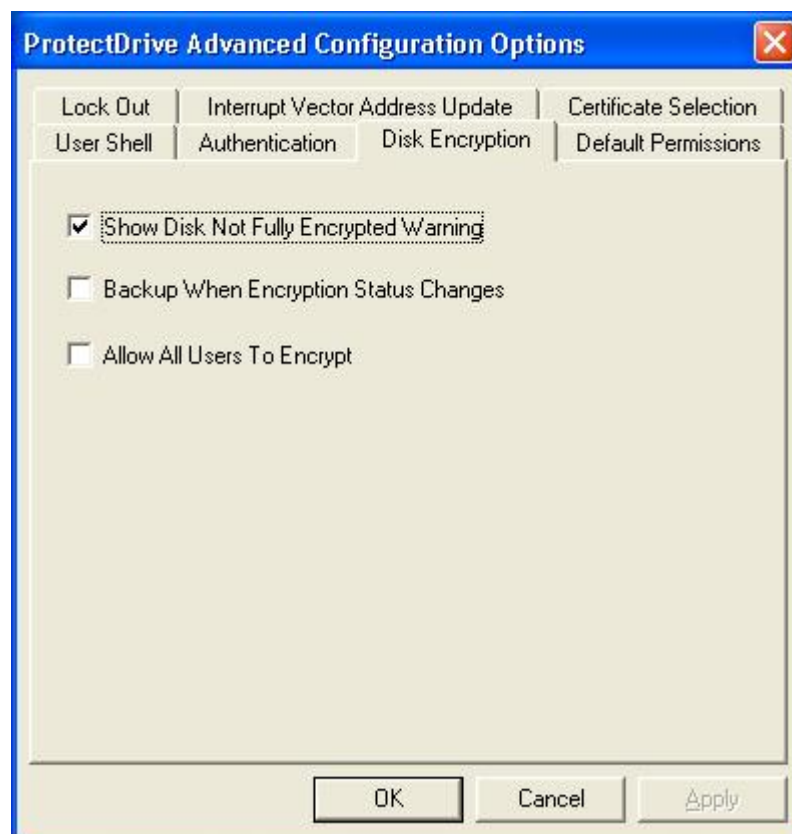
Allow Windows Logon Recovery

This option allows a user to automatically log on to their Windows account after exercising User Key Recovery. If enabled, the password recovery feature will store the encrypted user passwords in its user database. While the encryption is strong, this could be considered a security risk in certain environments.

Allow New User Introduction

This option is only available for password users (i.e., Local Users and Password Domain Users). If enabled, the user will be able to invoke the New User Introduction mechanism to retrieve a one-off access code from an Administrator to gain access to the system from the pre-boot logon. See CHAPTER 10 for more details on this option.

Disk Encryption Tab



Show Disk Not Fully Encrypted Warning

This option controls whether a warning message is displayed after logon when one or more disks are not fully encrypted.

Backup When Encryption Status Changes

This option controls whether the user will be prompted to backup ProtectDrive system files after encrypting or decrypting hard drives. If this option is set, the user will be prompted to backup system files the next time Crypdisk is run.

Note: The disk encryption key is stored in encrypted form in a ProtectDrive system file. If this system file becomes corrupted or lost due to system malfunction, the system cannot be decrypted without these backed up system files.

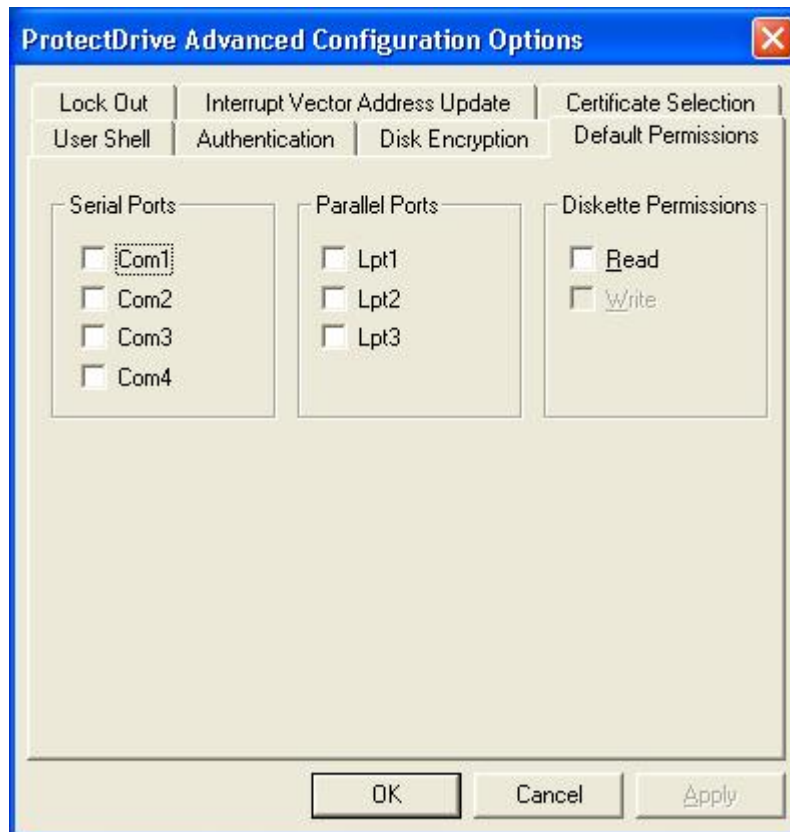
It is strongly recommended system files be backed up after the initial disk encryption to ensure systems are recoverable, if required.

Allow All Users To Encrypt

This option is currently unused.

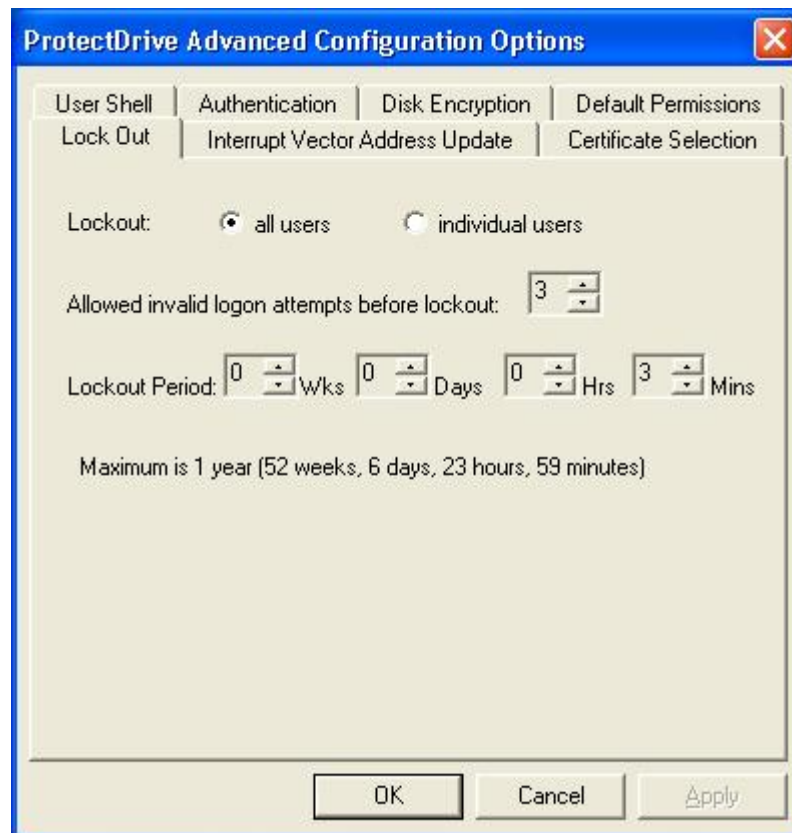
Default Permissions Tab

These permissions will apply to every user added to the ProtectDrive user database until they are updated via User Manager, for local users, or the ProtectDrive Active Directory snap-in for domain users.



Lock Out Tab

The lock out feature is designed to prevent password guessing attacks. After a number of failed logon attempts, further logon attempts are prevented for a configurable period of time.



Lockout All Users/ Individual Users

This setting determines whether access to all or individual user accounts is blocked for a period of time after too many failed logon attempts. The default is to lock out all user accounts.

Allowed Invalid Logon Attempts Before Lockout

ProtectDrive will lock a computer after the specified number of unsuccessful logon attempts at the pre-boot logon screen have occurred. The default value is three (3).

Lockout Period

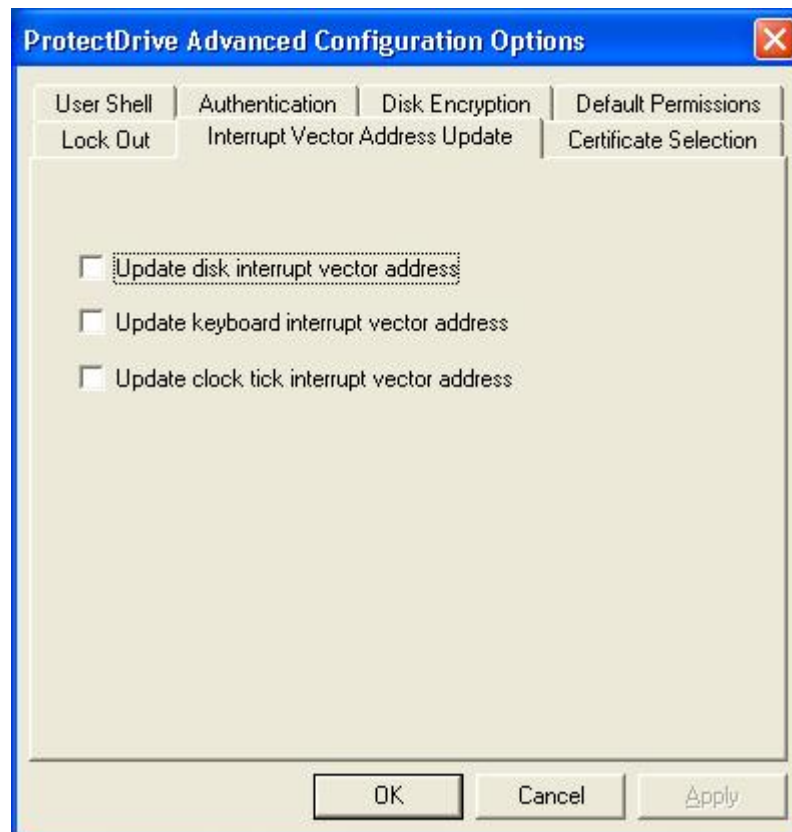
This value determines for how long access to the system or an individual account is blocked. The default setting is three (3) minutes.

A system that is locked can be unlocked by exercising the User Key Recovery challenge/ response mechanism, if this option is enabled.

Interrupt Vector Address Update Tab

ProtectDrive maintains a store of the BIOS interrupt vector addresses. This allows ProtectDrive to detect a potential attack mounted by changing an interrupt vector address. When ProtectDrive detects a difference between a BIOS interrupt vector address and the copy held by ProtectDrive, an error message is displayed.

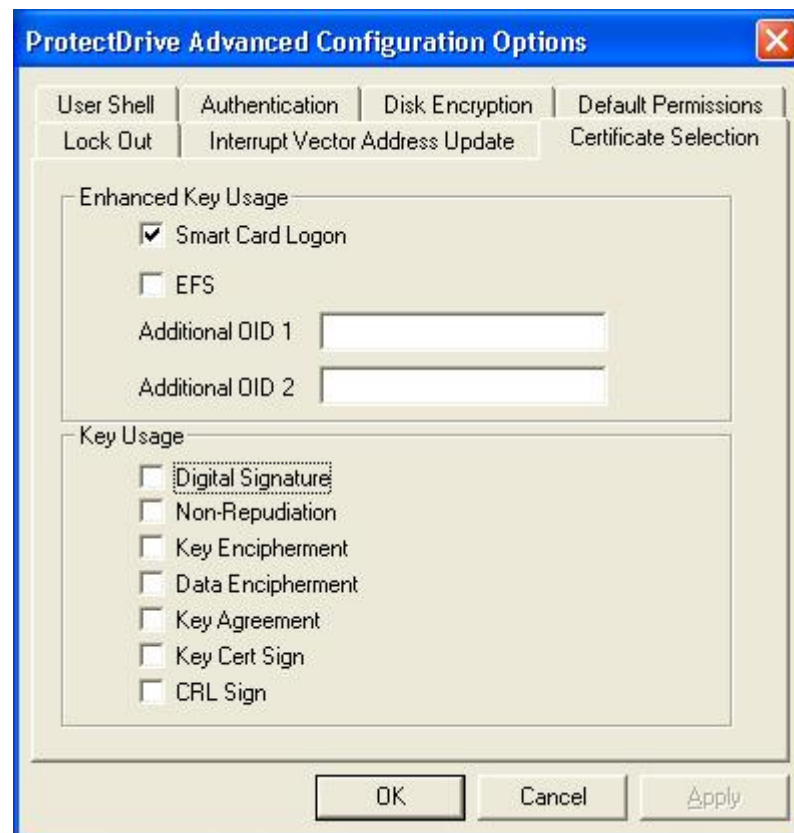
When interrupt vector addresses are changed by legitimate means (e.g. updating the BIOS), the error message is still displayed. The Interrupt Vector Address Update Tab provides a mechanism to accept a legitimate change by updating ProtectDrive's copy of the disk, keyboard, and clock tick interrupt vector address.



Check the vector address to update, and then click OK.

Certificate Selection Tab

This configuration tab is only relevant if two-factor authentication is used at pre-boot. These settings determine which certificates ProtectDrive will accept for this purpose.



By default, only the Microsoft Windows Smart Card Logon certificates will be used for pre-boot authentication.

Enhanced Key Usage

These settings define the Object Identifiers (OIDs) in the “Enhanced Key Usage” attribute of an X.509 certificate that need to be present for ProtectDrive to include the certificate in its user database.

If the “Smart Card Logon” checkbox is selected, certificates that include Smart Card Logon (1.3.6.1.4.1.311.20.2.2) in the “Enhanced Key Usage” field will be accepted by ProtectDrive.

If the “EFS” checkbox is selected, certificates that include Encrypting File System (1.3.6.1.4.1.311.10.3.4) in the “Enhanced Key Usage” field will be accepted by ProtectDrive.

Two additional OIDs can be specified to accept certificates that have other usages defined.

ProtectDrive accepts certificates that have **any** of the defined key usages.

Key Usage

The “Key Usage” field of an X.509 certificate represents a bit mask that defines the intended usage of the key (pair) associated with the certificate. Normally, selection of acceptable certificates via the Enhanced Key Usage attribute should be sufficient. To further narrow the range of certificates for use with ProtectDrive, the Key Usage can be specified here.

Note: Single Sign-On to Windows is only possible if the token used for pre-boot logon also contains a Windows Smart Card Logon certificate.

Note: ProtectDrive adds certificates on installation by querying Active Directory when users first log on to Windows with their token or when the `pduserdb.exe` is run. The settings defined here apply to all of the above methods.

CHAPTER 12

ProtectDrive and Networking

Network Installation

ProtectDrive provides installation options for roll outs to a large number of computers. The setup process can be automated such that all necessary setup files are stored in a central location accessible by client computers. Installation response files can be tailored to provide the options normally interactively selected by the installer. The use of an installation key file is a safe method for making the recovery key accessible in a shared directory during installation.

Please refer to the “ProtectDrive Network Installation Guide” for details of this process.

Local and Domain Accounts

When logging on to a Windows computer, users provide their username and password to access their account on the computer. They will then work on their Windows desktop, have separate areas where they store their files, and have certain privileges to modify settings or access system files or other users' files.

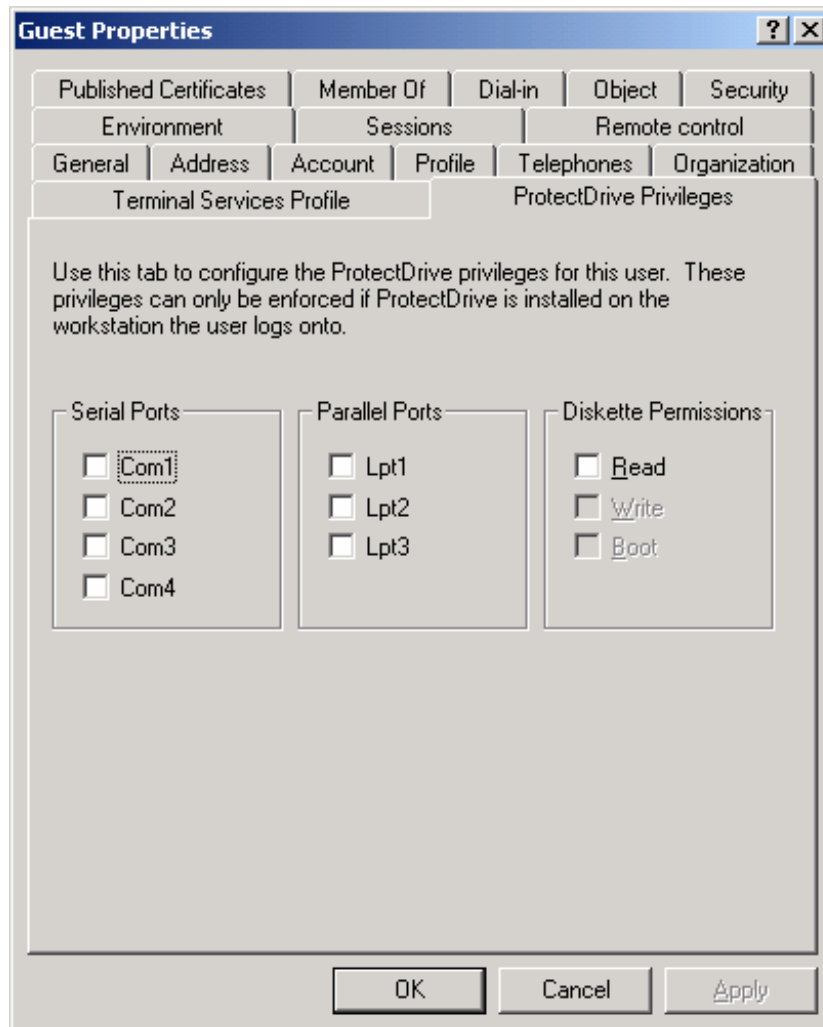
If the computer is part of a network and that network defines one or more domains, users also have to provide the name of the domain they wish to log on to. Selecting a domain from a drop-down list in the Windows logon screen does this. One of the options in this list contains the name of the local computer, which, when selected, logs the user into his or her account on the local machine.

Selecting a network domain will log the user into their domain account, which is an account that is different from their local account. Domain and local accounts are simply different accounts with different settings, different desktops, and, most likely, different user privileges.

ProtectDrive handles domain accounts in the pre-boot phase and will prompt the user to select a Windows domain or the local machine to log on. The information provided (username, password and domain or local machine name) at ProtectDrive logon is passed on to Windows logon, if Single Sign-On is configured. Only users with domain accounts can use a token to authenticate to ProtectDrive and Windows.

Server-Side User Management

- ProtectDrive provides an Active Directory server extension and a Microsoft Management Console snap-in for server-side administration of user privileges.
- This ProtectDrive Privilege tab looks and functions the same as the local user management extension as described in CHAPTER 16.



Each time a Domain User logs onto a machine, the Active Directory on the domain controller is contacted (subject to network connectivity) and the current ProtectDrive user privileges are updated.

Refer to CHAPTER 6 for details of the installation of the ProtectDrive server-side components.

CHAPTER 13

Recovery Administration

The Remote Recovery Administration utility RPADMIN.EXE is used for:

- Remote User Key Recovery
- Password fall back for Token Users
- New User Introduction

This utility implements a challenge/response protocol, which will either recover a user's forgotten password or grant one-off access to a computer secured with ProtectDrive.

These features are disabled by default and need to be explicitly enabled. See CHAPTER 6, Installation, and 0, Configuring ProtectDrive, for details about managing these options.

The user, from the pre-boot ProtectDrive logon screen, invokes one of the above procedures and will be presented with a screen displaying a thirteen character long challenge. In addition, the installation's serial number, the username, and Windows domain are displayed.



The user will communicate (typically via telephone) the serial number and challenge to an Administrator. The Administrator will identify the user as a legitimate user of the system, and enter the challenge and serial number into the Remote Recovery Administration console. A response code will be displayed on the console and given to the user.

The user will then enter the response code in the password field of the logon screen.

If the code was entered correctly, ProtectDrive will allow access to the system.

Remote User Key Recovery

User Key recovery will only be available for a user after a successful logon to Windows (with the User Key Recovery feature enabled).

The user invokes this feature by pressing SHIFT - F10 after entering their name into the ProtectDrive logon screen and placing the cursor in the password field.

- The screen displays the recovery challenge.
- The user communicates the challenge to the Administrator.
- The Administrator communicates the calculated response to the user.
- The user enters the recovery code and presses the [Enter] key.

Note: After the user key recovery is exercised, the user must change their password the next time they log on to Windows.

Password Fallback for Token Users

The user invokes this feature by pressing SHIFT – F9 at the PIN entry screen.

- The screen displays the password fallback challenge.
- The user communicates the challenge to the Administrator.
- The Administrator communicates the access code to the user.
- The user enters the recovery code and presses the [Enter] key. The operating system will be loaded.
- The Windows logon prompt will be displayed.
 - The user can logon with a newly issued token and this new token will be added to the ProtectDrive database. After the next reboot, this new token can be used to perform pre-boot authentication.
 - If no new token is available, the Windows Administrator has to ensure that username/password logon is enabled for this user.

The user can then enter their username and password to log on to Windows. This username and password combination will not be added to the ProtectDrive database.

Note: This feature is intended for emergency access in case of a misplaced token only.

New User Introduction

New Token Users are introduced by exercising the password fallback feature described above.

Users logging on with their username, password, and domain can be allowed through the ProtectDrive pre-boot authentication using the new user introduction. The user invokes this feature by pressing SHIFT – F9 with the cursor located in the User ID field.

- The screen displays the new user challenge.
- The user communicates the challenge to the Administrator.
- The Administrator communicates the response code to the user.
- The user enters the recovery code and presses the [Enter] key. The operating system will be loaded.
- The Windows logon prompt will be displayed and the user can enter their username and password to log into their local or domain account. This account will now be added to the ProtectDrive database.

Remote Recovery Administration Console

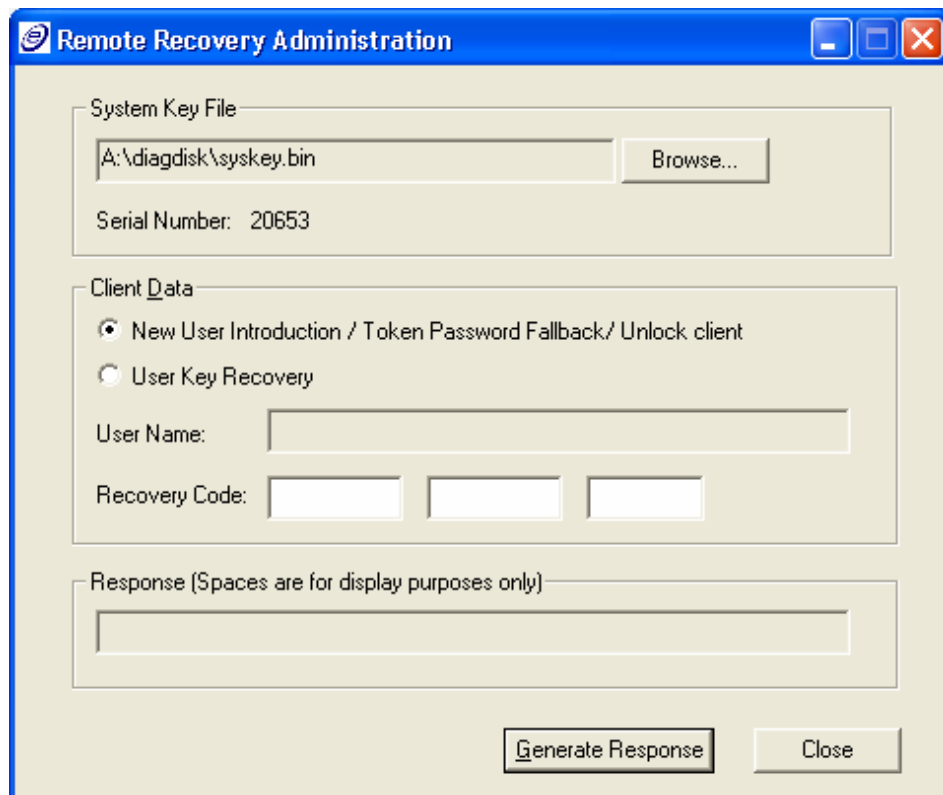
The Remote Recovery Administration Console is used to generate the response to the user's challenge, which will allow the user to log on to a system protected by ProtectDrive, if their logon credentials are unavailable.

The console (RPADMIN.EXE) is located in the "Recovery " folder on the ProtectDrive installation CD.

To generate the response to a challenge, the console requires access to the recovery disk matching the serial number of the system the user needs to get access to.

Note: The recovery files should NOT be copied off the recovery disk in order to avoid compromising an installation's security, even if it appears convenient.

When starting the password administration console, a file selection dialog will be displayed and allows the Administrator to select the correct Recovery Key File (`Syskey.bin`). The main console window will now displayed.



The screenshot shows the 'Remote Recovery Administration' window. It has a blue title bar with the text 'Remote Recovery Administration' and standard window controls. The main area is divided into three sections. The first section, 'System Key File', contains a text box with the path 'A:\diagdisk\syskey.bin' and a 'Browse...' button. Below this is a label 'Serial Number:' followed by the value '20653'. The second section, 'Client Data', contains two radio buttons: 'New User Introduction / Token Password Fallback / Unlock client' (which is selected) and 'User Key Recovery'. Below these are a 'User Name:' text box and a 'Recovery Code:' field consisting of three separate text boxes. The third section, 'Response (Spaces are for display purposes only)', contains a large text box. At the bottom right are two buttons: 'Generate Response' and 'Close'.

Using the [Browse] button, the Administrator can select a different system key, if required. The corresponding serial number can be compared with the one displayed on the user's challenge screen. Only if the serial numbers match will the challenge and response match.

Enter Challenges

The Administrator enters the challenge code generated by the user in the "Recovery Code" fields.

User Key Recovery

For a User Key recovery challenge, the Administrator enters the user's name in the "User Name" field. After entering the challenge in the "Recovery Code" field and selecting [Generate Response], the response to the challenge is displayed in the "Response" field.

Password Fallback and New User Introduction

The Administrator selects the New User option. After entering the challenge in the "Recovery Code" field and selecting [Generate Response], the user's access code is displayed in the "Response" field.

CHAPTER 14

Recovery Tools

ProtectDrive provides a number of DOS programs that can recover an unbootable or corrupt system.

A system may be unbootable for the simple reason that the user has forgotten their password and a mechanism to allow for recovery in this situation was not selected during installation. In this case, the ProtectDrive data files are intact and can be used by the recovery tools.

A corrupt system may be the result of disk failure. In this case, it is possible the recovery tools will require the recovery data files created by a backup process as the ProtectDrive file system on the hard disk may be inaccessible.

Location of Recovery Tools

The recovery tools reside in the “Recovery” directory on the installation CD. It is recommended that the contents of the “Recovery” directory be copied to the Registration Diskette and always be kept up to date with the latest version.

The following tools are provided with this version of ProtectDrive:

BACKUP.EXE
RMBR.EXE
DECDISK.EXE
DISPEFS.EXE

Using Recovery Tools

Boot the computer directly to a DOS Boot diskette or bootable CD.

Insert the diskette, or other medium, that contains the recovery tools. Some tools also require access to files on the Registration Diskette.

Run the recovery tool with `/?` to view the usage statement.

Command line options are prefixed with a ‘-’ or a ‘\’. A space is required between the option and any required data.

Using Recovery Data Files

The Backup.exe tool, or the optional backup that takes place each time the encryption status of the disk changes, creates a set of files that the recovery tools can work with should the disk become so corrupt that the ProtectDrive embedded file system is inaccessible.

Recovery Tools

RMBR.EXE

The Master Boot Loader (MBL) is a small program that is the first to be run when a computer is booting up. ProtectDrive modifies part of this file (the MBR) during installation to enable location of the embedded ProtectDrive file system prior to other disk access. If the MBL is replaced or corrupted after ProtectDrive installation, this tool will recover it.

Restoring the ProtectDrive MBR requires a sector by sector search of the boot partition looking for the ProtectDrive embedded file system. When found, the ProtectDrive MBR can be restored.

Replacing the original MBR is the same as running `fdisk /mbr`.

RMBR Command Line

Argument Syntax	Meaning
-?, /usage	Display the possible command line arguments
-v, /ver	Display version information
-p, /pd	Recover the ProtectDrive MBR
-o, /original	Recover the original MBR
-r, /recovery	Use recovery data files for either of the above options.

Current MBR Check

Prior to performing any tasks, RMBR will read the current MBR and display whether or not it is the modified ProtectDrive MBR. If it is, the following will be displayed:

```
Current MBR is the ProtectDrive MBR
```

If not, the following will be displayed:

```
Current MBR is not the ProtectDrive MBR
```

Version Checking Option -v

RMBR will attempt to verify it is working with the correct version of ProtectDrive. If the version is incorrect, the following will be displayed:

```
Incompatible versions
ProtectDrive Version:  7.1.0
rmbdr.exe Version:
```

Sometimes it is not possible to determine the version of the installed system.

Restoring the ProtectDrive MBR

RMBR -p

RMBR will first display a list of ProtectDrive partitions. Select the partition you wish to recover the ProtectDrive MBR for.

```
Disk  Start Sector      End Sector  Megabytes  Type...
1      63              16771859    8189        Primary (Boot)
(ProtectDrive)
```

```
Select partition to recovery. (Ctrl-C to exit) _
Current MBR is not the ProtectDrive MBR
Searching for super block from sector 63 to sector 20487599
99.99% and 3hrs 20mins remaining. (Press Ctrl C to stop)
```

RMBR will search the disk sector by sector looking for the ProtectDrive super block, which indicates the start of the ProtectDrive file system. It is possible that remnants from previous ProtectDrive installations exist on the drive. If a superblock is found but is not the super block for current installation, the following will be displayed:

```
Found super block at sector 1893443
Incorrect super block. Continuing search ..
```

If a valid super block is located, RMBR will display the version and ask for user verification, as shown below.

```
Found super block at sector 1893443
ProtectDrive v7.1.0
Is this the correct version of ProtectDrive? [Y/N]
```

If the version is not correct, enter N and RMBR will continue. If the version is correct, enter Y and the following will be displayed.

```
ProtectDrive MBR restored.
Current MBR is the ProtectDrive MBR.
```

Restoring the Original MBR

RMBR -o

This option replaces the current MBR with the MBR ProtectDrive saved during installation. Only do this if there are no encrypted drives.

DECDISK.EXE

This tool is used to decrypt any encrypted drives. Only use this tool when it is not possible to boot to the operating system and run the 32bit decryption utility.

DECDISK Command Line

DECDISK is able to run in a number of different ways. Use the command line parameters to specify how to run.

Argument Syntax	Meaning	Default Value
-?, /usage	Usage information.	
-v, /ver	Display version information.	
-kp, /keypath	Recovery Disk Path.	Current directory.
-r, /recover	Use recovery files to decrypt.	
-rp, /recpath	Path to recovery files.	Current directory.
-a, /all	Decrypt all encrypted partitions.	User selection.
-e, /est	Estimate region to decrypt.	

Decrypting Specified Partitions

DECDISK will first display partition information for all known partitions. The output will be similar to that below.

Partition Information

Disk	Start Sector	End Sector	Megabytes	Type...
1	63	16771859	8189	Primary (Boot)
1	16771923	78140159	29964	Logical
2	63	417689	203	Primary
2	417690	10217339	4784	Primary
2	10217403	12498569	1113	Logical

Area	Disk	Start Sector	End Sector	Algorithm	Megabytes
	% Enc'd	Type			
1.	1 63	16771859	3DES CBC	8189	
	100.00	Primary			
2.	2 6771923	78140159	3DES CBC	29964	
	100.00	Logical			
3.	2 63	417689	3DES CBC	203	
	100.00	Primary			
4.	2 417690	10217339	3DES CBC	4784	
	100.00	Primary			
5	2 10217403	12498569	3DES CBC	1113	
	100.00	Logical			

Select encrypted area to decrypt. (Ctrl-C to exit) _

DECDISK displays information on all the partitions. *Disk* is the physical disk number. *Start Sector* and *End Sector* are relative to the start of the physical disk. Next, DECDISK displays information on encrypted partitions. *Start Sector* and *End Sector* shows the extent of the encryption. The value in *Area* is used to select which area to decrypt.

The information above portrays two physical disks, the first with a primary partition and an extended partition that contains one logical drive. The second disk contains two primary partitions and an extended partition containing one logical drive. All partitions on the disks are fully encrypted with triple DES.

The user is required to select one of the encrypted areas to decrypt. As the decryption progresses, the user is informed of the percentage of the encrypted area still to be decrypted and approximately, how long that will take.

```
75.10%          3hrs:15mins remaining (Press Ctrl-C to stop)
```

Once the decryption is complete, the list of encrypted areas will be refreshed. When there are no more encrypted areas, the following will be displayed.

```
No encrypted areas found.
```

Using the Recovery Data Files

In case of serious system corruption, the ProtectDrive files may not be available on the installation drive. DECDISK requires Recovery Data Files under this condition.

Note: Recovery Data Files are created only if the backup option was enabled during installation or the BACKUP.EXE tool has been run after the most recent disk encryption operation.

```
decdisk -kp 1:\pd\key -r -rp 1:\pd\recover
```

The above example will allow the user to select which encrypted partitions to decrypt. The Syskey.bin file will be found in 1:\pd\key and the recovery data files found in 1:\pd\recover.

Entering an Area to decrypt Option -e

Serious system damages cause the Drive Table Entry file corrupted. DECDISK can decrypt the encrypted disk when the sector numbers of an area are available. DECDISK takes user input for the start and end sector and the algorithm.

```

Partition Information
Disk   Start Sector   End Sector   Megabytes   Type...
1      63              16771859    8189        Primary (Boot)

Enter disk number 1
Enter start sector 63
Enter end sector 16771859
Enter Alg (1=DES, 2 = 3DES, 3 = Idea) 3

-----
Area  Disk  Start Sector   End Sector Algorithm   Megabytes % Enc'd
1.    1      63              16771859    3DES CBC      8189      100.00

Select encrypted area to decrypt. (Ctrl-C to exit) _

```

DISPEFS.EXE

This tool displays contents of important ProtectDrive files. It is a diagnostic tool rather than a recovery tool.

ProtectDrive stores its data in a number of files contained in an Embedded File System (EFS). DISPEFS enables users to display the contents of some of the EFS files.

Argument Syntax	Meaning
-?, /usage	Display the possible command line arguments.
-v, /ver	Display version information.
-a, /all	Display all files.
-d, /dtes	Display drive table entries
-c, /cfg	Display configuration data
-g, /gda	Display general data
-d, /dky	Display key data.
-x, /ex	Display exchange data.
-u, /user	Display the user database.
-r, /rec	Display from recovery data files
-rp, /recpath	Path to recovery data files
No Arguments	Display all files.

The output of dispefs.exe can be captured to another file by running the following command:

```
dispefs [Command Line Arguments] > outefs.txt
```

BACKUP.EXE

This tool creates ProtectDrive recovery data files. All of the recovery tools are able to function with the files created by this tool. This is very

useful when the disk is corrupt and the ProtectDrive file system is inaccessible. This tool creates the same set of files that are optionally backed up when the encryption status of the drive changes. It is imperative that these files are kept up to date.

Argument Syntax	Meaning	Default
? / usage	Display the possible command line arguments.	
v / ver	Display version information.	
t / tgt	Target directory for backup files.	Current directory.

The most important use of these files is to assist in recovering an encrypted corrupt drive. As the recovery data files indicate which areas of the disk are encrypted, it is important that only the most up-to-date version of these files are used.

The ProtectDrive programs that are able to change the encryption status of an installation, will, if the user selected the installation option to backup, prompt the user to backup when they finish.

If the installation option to backup data files was not selected, the user can do this at any time by running this program.

These files are machine specific and need to be kept for each machine.

Specifying a Target Directory

If running under Windows, the computer name is included automatically in the target path. For example, the following command line creates the recovery data files in *t:\recovery\M-WORK101*, where M-WORK101 is the computer name:

```
backup -tgt t:\recovery
```

When running from DOS, the computer name is not included in the target directory path, and the above command line would create the recovery data files in *t:\recovery*.

PDUSERDB.EXE

This command line tool to manipulate the ProtectDrive pre-boot user Database allows an administrator to:

- List the names of users authorized to perform ProtectDrive pre-boot authentication.
- Remove local and domain accounts from the ProtectDrive user database.
- Add local and domain accounts to the ProtectDrive user database.
- Change a user's password.

Argument Syntax	Meaning	Default
? / usage	Display the possible command line arguments.	
l/ list	Display the list of ProtectDrive users.	
r/ remove	Remove a ProtectDrive user	
a/ add	Add a ProtectDrive user	
c/ change	Change Password for a ProtectDrive user	
n/ name	Username of the user to be added or removed	
p/ password	Password of the user to be added	
d/domain	Name of the domain the user is associated with	Local machine

Adding a user

To enable a user to successfully authenticate at pre-boot time, the user credentials can be added to the ProtectDrive user database as follows:

For password accounts:

```
pduserdb -a -n username -p password -d domain
```

For token accounts:

```
pduserdb -a -f filename -n username -d domain
```

where filename is the name of a file containing the user's DER encoded X.509 certificate.

Removing a user

If users should not be able to access a machine protected by ProtectDrive any longer, they can be removed from the ProtectDrive user database as follows:

For password accounts:

```
pduserdb -r -n username -d domain
```

For token accounts:

```
pduserdb -r -f filename -n username -d domain
```

where `filename` is the name of a file containing the user's DER encoded X.509 certificate.

Note: In this version of `pduserdb`, the built-in user can be deleted with this function as well. Consequently, it is possible to delete all users from the ProtectDrive user database, which will make it impossible to boot a protected system without recovery action (e.g., decrypting the system disk with the `decdisk` recovery tool). Administrators need to be aware of this possibility and ensure that at least one user with available credentials remains in the user database to enable successful pre-boot authentication.

Changing a user's password

To change a user's pre-boot password:

```
pduserdb -c -n username -d domainname -p new_password -o  
old_password
```

CHAPTER 15

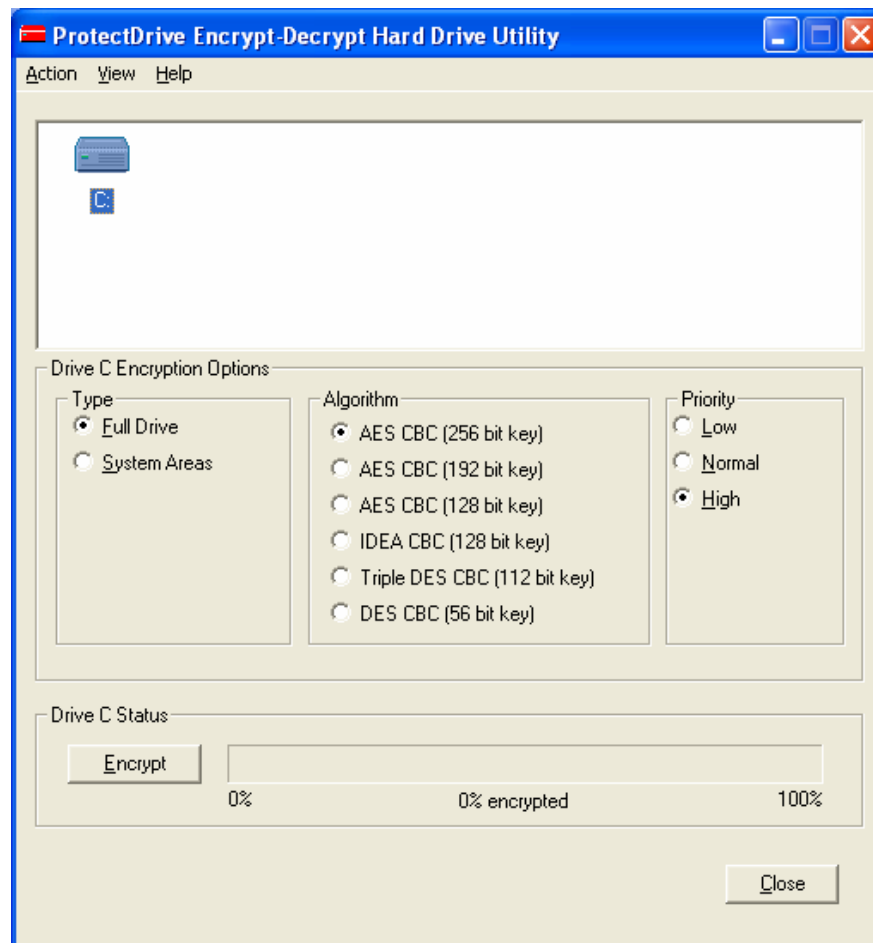
Encrypt-Decrypt Hard Drives

Using Crypdisk

The Crypdisk utility can be used to encrypt or decrypt selected drives. One or more drives can be selected for either encryption or decryption. Optionally, only the system areas of the nominated partition can be encrypted if desired. This would provide excellent performance but leave most data on the partition unencrypted.

When Crypdisk is first started, two Advanced Configuration Options are checked. The first option is the backup option on the Disk Encryption page. If this is set and the disk encryption status of the disk has changed but a backup has not been made, Crypdisk will prompt the user to backup now.

The second option controls whether users without administrative privilege are allowed to initiate disk encryption ("Allow All Users To Encrypt"). If this option is not set and a user without administrative privilege attempts to initiate disk encryption, a corresponding message is displayed and Crypdisk terminates.



Encrypting Multiple Drives

More than one drive can be selected for encryption or decryption.

SHIFT - select	will select a sequence of drives.
CTRL - select	allows selection of individual drives.

If one drive is partially encrypted and the sequence terminated, operations will always start on that drive.

Encryption Algorithm Selection

The selection presented depends on the algorithm group chosen during installation.

DES Cipher

The DES cipher is a publicly tested 56-bit key 64-bit block cipher. ProtectDrive operates this cipher in CBC Mode. Details on the cipher are publicly available from many sources.

Triple DES Cipher

The Triple DES cipher is a publicly tested 112 bit key 64 bit block cipher. ProtectDrive operates this cipher in CBC mode. Details on the cipher are publicly available from many sources.

IDEA

The International Data Encryption Algorithm (IDEA) was developed in the early 1990s. It operates using 64-bit blocks and 128-bit keys. ProtectDrive uses the cipher in CBC mode.

AES

The Advanced Encryption Standard was announced by NIST in November 2001 in FIPS PUB 197. It is symmetric block cipher that processes 128-bit data blocks and uses 128-bit, 192-bit, or 256-bit keys. ProtectDrive uses the cipher in CBC mode.

Disk Encryption Security Warning

ProtectDrive is only fully secure once all partitions on all hard drives are fully encrypted. If one or more drives are not fully encrypted, a warning message can be displayed to notify users of this security weakness.

To show this warning, the “Show Disk Not Fully Encrypted Warning” in the Advanced Options Dialog must be checked. By default, this warning is enabled.

Security Warning



If any drives are found to be unencrypted, a warning message similar to the one below will be displayed in order to notify the users of this security weakness.

Provided this warning has not been disabled, it will be displayed after every login.

A ProtectDrive System Administrator can turn off this warning by using the “Show this warning next time?” checkbox in the warning screen.

Drive Selection

All drives that can be found and possibly encrypted will be displayed. The icon used to represent the drive indicates whether the drive is:



decrypted



partially encrypted or decrypted



encrypted

When a drive is selected, information pertaining to that drive will be displayed in the Options and Status boxes.

Multiple drives can be selected for the same cipher operation only (i.e., drives to be encrypted cannot be selected with drives that require decryption).

Once a drive has been partially encrypted or decrypted, it will not be possible to de-select that drive until the partial operation has been completed. It is possible to select additional drives requiring the same cipher operation.

If multiple drives are selected for encryption, they will all use the encryption options specified prior to the user clicking on the [Encrypt] button.

For decryption operations, ProtectDrive will automatically detect the appropriate algorithm.

System Areas Only

Selecting “System Areas Only” when encrypting implies only the system areas of the selected partition will be encrypted and the data areas will be left unencrypted. This provides a lower level of security with increased performance. From an unauthorized floppy boot, data may be seen with disk edit type programs but the partition will not be visible as a valid file system.

Priority Selection

When drives are being encrypted/decrypted, whichever Priority Selection setting you chose affects the encryption process. The recommended setting is High, which uses the largest block size for the encryption process and produces the shortest time for the operation.

Priority - Low

The encryption task will operate with small blocks of data being encrypted at a time to reduce the impact on the performance of other tasks that may be active in the system. The user will have better interactive response. At this setting, the disk encryption operation will take more time to complete than if the setting was normal or high.

Priority - Normal

The encryption task will operate with medium-sized blocks of data being encrypted at a time to reduce the impact on the performance of other tasks that may be active in the system. The user will have reasonable interactive response. At this setting, the disk encryption operation will take more time to complete than if the setting was set to high.

Priority - High

The encryption task will operate with larger blocks of data being encrypted at a time. This may have a greater impact on the performance of other tasks that may be active in the system. The user will have poorer interactive response. At this setting, the disk encryption operation will be completed in the shortest possible time.

Encryption

Once the settings are as required, click on the [Encrypt] button to start the operation. If multiple drives have been selected, they will be encrypted one after the other.

During the operation, Crypdisk will indicate the progress of each drive via the percentage complete bar and give a time remaining indicator. Once started, the operation may be stopped at any time by pressing the STOP button, and restarted by pressing START. Note that it will not be possible to perform other encrypt or decrypt operations on a partially encrypted or decrypted drive until the selected operation has completed successfully.

The system is fully re-startable. This means half of the “a” partition could be safely encrypted one day and the operation completed the next day. The system can be used normally while the encryption operation is being carried out.

Note: Power failure may cause data corruption. You should backup your data before starting a disk encryption.

Decryption

The only option able to be changed for decryption operations is the priority. The algorithm used for the decryption will be the same that was used for the encryption. If the drive had a Systems Area Only decryption then that is all that will be decrypted.

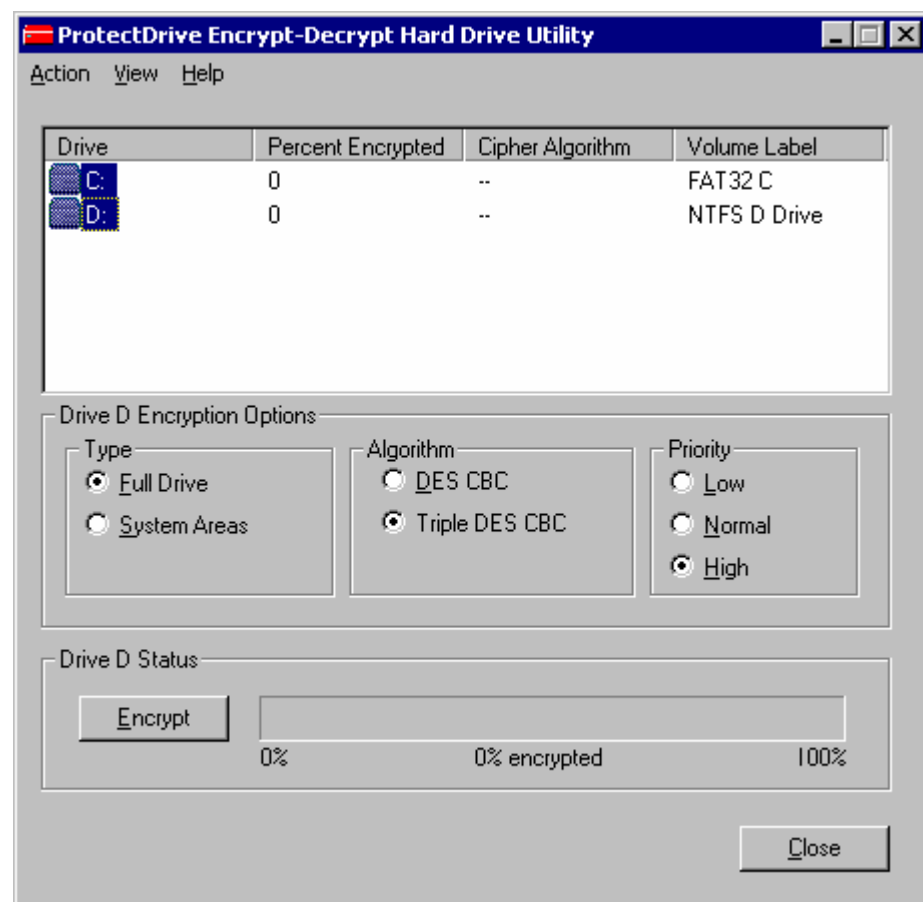
Any number of drives requiring decryption can be selected, and the process for all the selected drives started by clicking on the [Decrypt] button. At any time the operation may be stopped and restarted. It is not possible to encrypt or decrypt other partitions while any partition remains partially encrypted or decrypted.

As the decryption operation is a security concern, this operation requires the recovery or registration disk used to install the system and the user must have Administrator privileges.

Note: Power failure may cause data corruption if it occurs during the decryption process.

List View

Selecting the "List" option from the "View" menu displays the current encryption status of all drives and partitions.



Note: When using ProtectDrive, always assign a meaningful label to all partitions, which will be displayed in the "Volume Label" field. This will prove valuable if it is necessary to decrypt using the recovery tools (See CHAPTER 13), and when the Multi-Boot version is being used.

Command Line Options

The `crypdisk.exe` also has a command line interface, which is used in automated network installations to perform the initial encryption of hard disks. In this case, the encryption configuration is read from a response file.

Command Line Arguments:

- c Run in non-interactive mode
- r file Response file for non-interactive mode.
- l file Logfile (mandatory for non-interactive mode)
- s X Return encryption status of drive X as program return code
 (0 = fully encrypted, > 0 = not fully encrypted or unencrypted)
- h Display usage information

Determining the Encryption Status of a Disk

The following batch program uses the **crypdisk** program to determine whether a hard drive is fully encrypted or not.

```
C:\securdisk\binnt\crypdisk -s%1
if %ERRORLEVEL% == 0 goto isEncrypted
goto isNotEncrypted

:isEncrypted
echo %1 is fully ENCRYPTED
goto end

:isNotEncrypted
echo %1 is NOT fully encrypted
:end
```


Backing up

ProtectDrive provides a set of recovery tools which, in case of system corruption, can utilize the system files backed up by Crypdisk. As some of the files contain information relating to the encryption status of the system drives, it is important that they be kept up to date.

When Crypdisk is closed and the encryption status of the drives has changed, a message box prompting the user to backup is displayed.

If the user selects [OK], a directory selection dialog is displayed and the ProtectDrive system files will be backed up.

If the user selects [Cancel], a flag will be set and users will be prompted to backup each time the system is restarted or the next time Crypdisk is run.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 16

User Management

User Database Management

During installation, ProtectDrive creates a user database where permissions and attributes are stored. This database is synchronized with the local Windows user database, if this option is enabled. The installer can optionally view this database at the time of installation. Subsequently, any changes to users will automatically be synchronized.

An additional level of control over user permissions and attributes is available when ProtectDrive is installed from a network. A "Configuration Response File" can be used to establish new users and set existing ones. The applicable rules are described below. Note that when a Configuration Response File is used, a log file is produced in order to check that the new database has been synchronized.

Introducing New Users

If synchronization with the local Windows user database during installation is disabled, local Windows users cannot log on at pre-boot time (with the exception of the user installing the product, if they are a local user). To allow access to the machine, an authorized user has to log on at pre-boot time. The local users can then enter their user credentials at the Windows logon prompt and will be added to the ProtectDrive user database. Alternatively, the "New User Introduction" challenge/ response protocol as described in CHAPTER 10 can be exercised to allow users access to a machine.

User Privileges

To simplify user management under Windows, a Windows Administrator is automatically assigned as a ProtectDrive Administrator. Administrator privilege is granted and denied using standard Windows means.

ProtectDrive recognizes two types of users as shown below:

Administrators

An Administrator (including the built-in Administrator) can modify privileges, access permissions and passwords for all ProtectDrive users, with the exception that they are not able to modify the access permissions for any Administrator.

Administrators are responsible for setting their own access permissions.

The Built-in Administrator created during Setup is a ProtectDrive Administrator whose account cannot be deleted or modified.

End Users

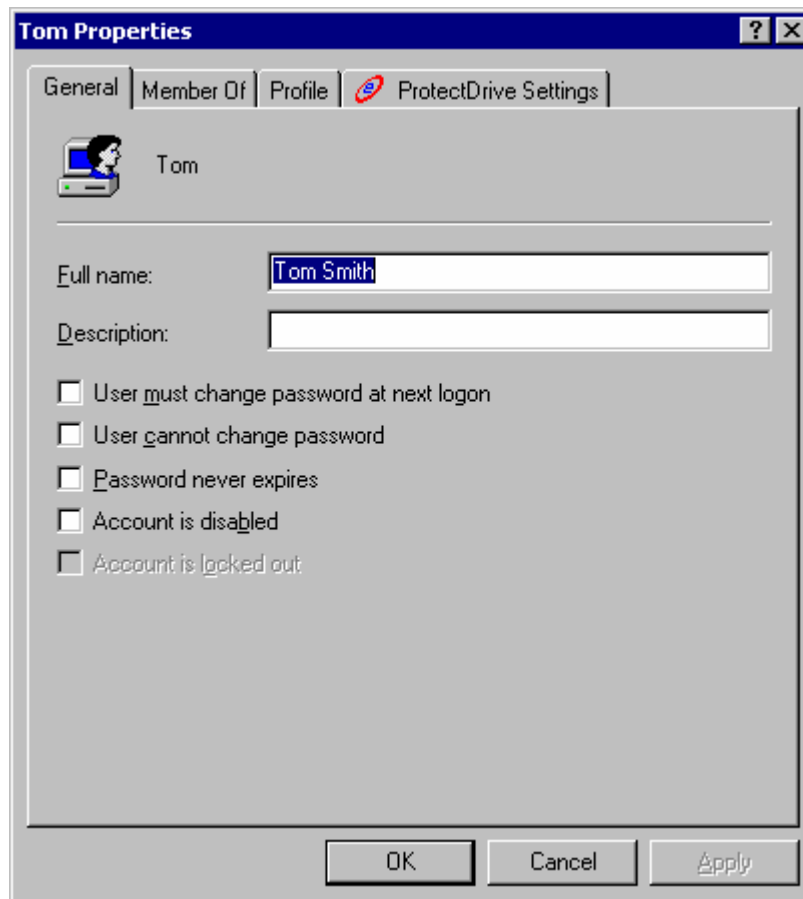
End Users cannot modify their own or anyone else's privileges and access permissions. They are able to change their password as normal.

User Properties

To add, delete, or modify users, run the Windows User Manager program accessed through Start/Programs/Administrative Tools/User Manager (or User Manager for Domains), or the Windows 2000 User Management, accessed through Computer Management.

Select the user or group of users you wish to act on and select User Properties from the User menu.

When the User Properties window is displayed, a ProtectDrive tab is displayed. Select this tab to set users' access permissions.



Note: After ProtectDrive is installed, it is no longer possible to delete the currently logged on user since this would invalidate the credentials used to give access to disk decryption. To delete a user account, an Administrator needs to log on to Windows and remove the account.

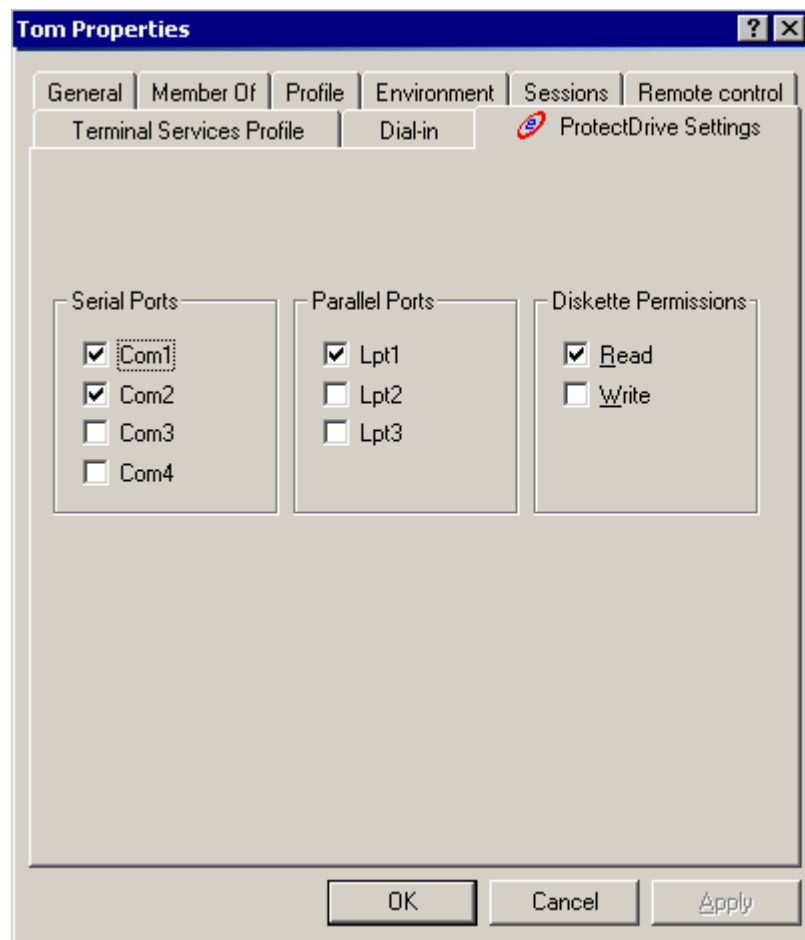
Username

Username are not considered confidential information in the ProtectDrive system. Therefore, it is common for first names and/or initials to be used as the username. This is standard practice and should not be construed as a security risk. Both Windows and ProtectDrive usernames have a maximum length of twenty (20) characters.

Privileges and Access Permissions

The settings shown in the following diagram indicate a user with access to serial and parallel ports, and read access to floppy diskettes.

Port Access permission checkboxes are shown for supported serial and parallel ports. Checking a box allows access to the port, otherwise the selected users will not be able to access the port.



If a mouse is connected to the port, ProtectDrive is unable to deny access to this port.

Diskette Permissions

This section controls the user's access to the various diskette operations. Checking a box enables the particular operation and clearing the box disables it.

- **Read** - allows the user read access permission to the diskette drives of the PC. Users are normally denied read access to prevent the unauthorized importation of software and data. This control can also prevent the importation of virus-infected programs.
- **Write** - allows the user write access permission to the diskette drives of the PC. Users are normally denied write access to prevent the unauthorized exportation of software and data. Write permission includes read permission and gives the user the ability to format diskettes.

CHAPTER 17

Passwords

System Chosen Passwords

System-chosen user passwords can be very secure and can resist password guessing attacks since the system software or the Administrator can enforce a set of rules that will create passwords, which are highly resistant to attack.

System-chosen user passwords tend to be more insecure as they are generally difficult for the user to remember and, therefore, often recorded (e.g., on a Post-it Note) in some form that makes their disclosure possible.

User Chosen Passwords

User-chosen passwords can be secure, as they can be constructed in a way that is easy to remember and, therefore, will not have to be recorded. User-chosen passwords can also be very insecure, as users often select easy to guess passwords, such as their names or other personal information.

Password Security

A user's password is confidential information in the ProtectDrive system, and it should be treated as such in normal circumstances. A user's password should not be disclosed to other users or recorded in any form whatsoever.

Password Strength Enforcement

ProtectDrive password strength enforcement may be disabled at installation, by default it is enabled. When enabled, ProtectDrive uses the following enforcement and restrictions to help maintain high strength passwords on the PC:

- Passwords may never be less than the configured minimum (default of six) characters in length.
- User passwords must not be the same as the Username.
- User passwords must not be the same as the Domain name.
- Passwords cannot have more than two (2) consecutive identical characters.
- Password history is maintained so that recently used passwords cannot be reused.

Choosing Passwords

As the ProtectDrive system has been designed for personal computers, the following major points should be noted:

- System-generated user passwords are often forgotten and tend to be recorded by the user in a non-secure form.
- ProtectDrive and Windows have built-in facilities that provide measures to improve the strength of user-chosen passwords.
- ProtectDrive provides measures to resist password-guessing attacks.

With these points and others in mind, ProtectDrive and Windows implement a password system where the users choose their own passwords.

A List of Don'ts for Choosing Passwords:

- Don't use the logon name, first, or last name in any form (reversed, capitalized, doubled, etc). ProtectDrive will refuse a password identical to the username.
- Don't use partner's, relatives, or children's names.
- Don't use easily obtainable personal information, such as a telephone number, street name, street number, car registration number, birth dates, or the date of a significant historical event.
- Don't use confidential personal information, such as a PIN number, TAX file number, etc.
- Don't use keyboard scales (e.g., qwerty or asdfgh).

A List of Do's for Choosing Passwords:

- Use a phrase that is easy to remember instead of a word such as 'Once upon a time.'
- Use two short words concatenated with punctuation marks, such as 'Coffee+Time' or 'Good,Sport'.
- Use the first letter in each word of a phrase (poem or song) to make a nonsense word (e.g., 'On the first day of Christmas' would become 'OtfdoC').
- Use a keyboard offset approach. That is, offset keys as a password is entered (e.g., fisher becomes godjrt)

Password Changing Restrictions

Windows may be configured to allow password changes only after a certain number of days have passed. This feature is highly recommended and should be used.

Password Aging

Windows provides a password-aging scheme to force users to regularly change passwords. If a user uses the same password for an extended amount of time, it may eventually be accidentally disclosed or obtained by casual observation. The password-aging scheme helps lessen this chance of password compromise. This feature should be enabled at all times.

Assigning Passwords to New Users

When an Administrator creates a new user, the Administrator assigns a temporary password for that user. The user may then logon to the system with the Administrator-chosen password. As mentioned above, the use of passwords chosen by an Administrator normally leads to the user recording the password in some form, which effectively compromises it. To overcome this problem, Windows can be configured to allow only a single (1) logon with the Administrator-chosen password, and a subsequent logon will require a password change.

Password History

Windows may be configured to retain password history information on every user. The password history data contains information on the most recent passwords employed by each user.

This allows the system to reject new passwords that have been used recently and lessens the chance of password compromise. It is recommended that this feature be enabled.

Lockout Feature

Windows has an account lockout feature, which should be used as part of the security system. Accounts are locked when a certain number of invalid attempts are made to logon with that account name. See Windows User Manager Documentation or On Line Help for information on using this feature.

Password Attacks

ProtectDrive monitors the number of unsuccessful logon attempts. If a successful logon is not achieved after a certain number of attempts, the system will inhibit any further attempts for a configurable period of time. Each subsequent unsuccessful attempt will incur a further delay. This is designed to effectively frustrate an out-of-hours password-guessing attack. The next successful logon will reset this system.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 18

Automatic Pre-Boot Authentication

Automatic Preboot Authentication can be configured by either using the **SETAUTOPBA.EXE** utility or by amending the Windows Registry. Registry amendments take priority over the settings implemented by **SETAUTOPBA.EXE**.

Using the SetAutoPBA Utility

Automatic pre-boot authentication can be configured using the **SETAUTOPBA.EXE** utility. This utility is more secure than the method outlined below under “Amending the Windows Registry.” This is due to the fact that the username and password used for automatic pre-boot authentication are stored in encrypted form in the ProtectDrive embedded file system. The utility can be found in the \SERVER directory on the ProtectDrive CD. It requires a password to be used at pre-boot, as well as other input arguments as shown below.

Usage: **SETAUTOPBA.EXE** [ARGUMENTS]

Arguments	Description
/d or /domain	Domain name to be used at pre-boot
/u or /user	User name to be used at pre-boot
/p or /password	Password to be used for automatic pre-boot authentication
/c or /count	Total number of allowed automatic authentications
/r or /reset	True or False, this is used to reset the Interrupt Vector Address in cases where they are modified

If the password is not specified on the command line (with the /p switch), the user running **SETAUTOPBA.EXE** will be prompted to enter and confirm the password interactively.

Amending the Windows Registry

After installation, ProtectDrive users are required to authenticate successfully to ProtectDrive before the operating system is loaded.

Since this authentication requires user interaction, it can become an obstacle to automated administrative tools, which require one or more unattended re-boots of the computer to complete their maintenance tasks.

To enable such tools, ProtectDrive provides a set of registry values, which can be used to configure automatic pre-boot authentication:

HKLM\Software\Eracom Technologies Australia Pty. Ltd\ProtectDrive\

Value	Type	Meaning
APB_Count	REG_DWORD	Number of automatic pre-boot authentications allowed. = 0: No automatic pre-boot N > 0: Allow N automatic pre-boot authentications. Note: this value will be reset to 0, if pre-boot authentication fails.
APB_Username	REG_SZ	Name of a valid Windows and ProtectDrive account. A successful Windows logon must have occurred before ProtectDrive is able to recognize this username. Note: The Windows account should subsequently be disabled in Windows before this feature is used.
APB_Password	REG_SZ	Password for the above account.
APB_Domain	REG_SZ	Domain name or local machine name that was used when the Windows logon for this account was performed.

HKLM\Software\Eracom Technologies Australia Pty. Ltd\ProtectDrive\

Value	Type	Meaning
APB_ResetIntVects	REG_DWORD	<p>ProtectDrive provides a protection mechanism that detects changes in interrupt service handler routines, memory size, etc., which may indicate that a system has been tampered with. If ProtectDrive detects such a change, a warning message is displayed after pre-boot authentication. This warning message can also be triggered by BIOS updates.</p> <p>This registry value provides a mechanism to suppress these warning messages when a system is updated in a controlled environment and the automatic pre-boot authentication is exercised. This value is optional and the warning message is suppressed if the value is set to 1.</p>

Setting Up Automatic Pre-Boot Authentication

The following is an example automatic pre-boot authentication configuration and the values to be entered (in **bold**) are indicative only:

Navigate to **Control Panel - Administrative Tools - Computer Management - Local Users and Groups** and create a Windows account to be used for pre-boot authentication. For example,

- Local account (computer name is **Computer**)Username **preboot**
- Password **password**
- Set the Windows account to disabled.

Open the registry and navigate to:

HKEY_LOCAL_MACHINE\SOFTWARE\Eracom Technologies Australia Pty. Ltd.\ProtectDrive.

- Create a DWORD-Value **APB_Count** and set the value to **2**.
- Create a String - Value **APB_Username** and set the value to **preboot**.
- Create a String - Value **APB_Password** and set the value to **password**.
- Create a String - Value **APB_Domain** and set the value to **Computer**.

Restart the computer.

The registry value `APB_Count` is decremented by one after every successful pre-boot authentication. If the counter reaches the value 0, all four values will be erased from the Registry.

If any of the details entered in the registry are incorrect and the automatic pre-boot authentication could not proceed, an error message is displayed. After the message is acknowledged, the normal interactive logon screen is displayed. In case of an unsuccessful pre-boot authentication, all pre-boot authentication configuration values in the Registry are erased.

Note: Using automatic pre-boot authentication circumvents an important ProtectDrive security mechanism. The password for a valid ProtectDrive user account is available in clear text in the Registry while this feature is in use. Thus, this feature should only be used for administrative tasks in known and controlled security environments.

CHAPTER 19

Token Initialization

ProtectDrive supports strong two-factor authentication at pre-boot time, which integrates tightly with the Windows smart card logon feature. If your organization already uses smart cards or tokens to logon users to Windows, this chapter can be skipped.

The only configuration step required is to allow token authentication during ProtectDrive installation. The ProtectDrive user database can be populated by selecting users and groups from Active Directory.

See CHAPTER 6 for details of enabling token authentication during ProtectDrive installation and CHAPTER 10, Logging On, for details of pre-boot token authentication.

Setting up Windows Smart Card Logon

Smart card support was integrated into Windows 2000 as a key component of Microsoft's public key infrastructure. A search on <http://search.microsoft.com> for "smart card logon" will return a number of useful resources that will enable you to set up smart card logon in Windows 2000 and XP.

Here are a number of key documents:

A white paper providing technical background information smart card logon.
--

Knowledge Base Article 257480 covers setting up the Certification Authority and enrolling user certificates.
--

A troubleshooting paper covers optimizations, errors, and fixes.
--

ProtectDrive requires that the Microsoft Certification Authority (CA) is used to enroll user certificates. Third-party CAs are not yet supported.

Note: The Microsoft CA needs to be set up as Enterprise CA.

Installing the Smartcard Runtime Environment

The smart card Runtime Environment (RTE) needs to be installed on

- all computers that are used to enroll certificates for users and
- all computers that will be secured by ProtectDrive and will use tokens to authenticate legitimate users.

The respective RTEs are available from the corresponding smart card manufacturers. The Aladdin eToken RTE, for example, is available for download from Aladdin's Web site at

<http://ealaddin.com/etoken/downloads/rte.asp>

Installing the RTE on a computer will automatically enable Windows smart card and token logon. This is indicated by a modified Windows logon dialog that prompts users to either insert their smart card or press Ctrl+Alt+Del to logon with their username and password.

Working with the Microsoft Management Console

The Microsoft Management Console (MMC) combines administrative tools that are used to administer your infrastructure, including networks, computers, users, and services.

The following paragraph is provided as an example only and needs to be tailored to the respective environment. Please refer to the Microsoft online help for further details.

Different administrative tasks are carried out via "snap-ins", which can be added to the Management Console.

- Select **Start / Run** and enter mmc .
- In the MMC, select **Console / Add/Remove Snap-in**.
- In the Add/Remove Snap-in dialog, select the **Standalone** tab and click **Add**. This will display a list of available snap-ins. Snap-ins are added individually:
 - Select **Active Directory Users and Computers** and click **Add**.
 - Select **Active Directory Sites and Services** and click **Add**.
 - Select **Certification Authority** and click **Add**.
Select "Local Computer", if the CA is running on the same machine and click **Finish**.
 - Select **Certificates** and click **Add**.
 - Select "My user account" to manage certificates for the administrator account currently logged in and click **Finish**.
- Click **Close** in the Add Standalone Snap-in dialog.
- Click **OK** in the **Add/Remove Snap-in** dialog.

- The MMC now shows the snap-ins selected.
- Select **Console / Save As**, enter a name for this MMC configuration and click **Save**.

This MMC instance will be added to the Start/ Administrative Tools menu of the current user.

Setting Up Smart Card Enrollment

This section lists the configuration steps to enable smart card enrollment in Enterprise CA. For details of each of these steps, refer to the relevant Microsoft documentation.

Configure Certificate Templates.

- Select **Certificate Authority** in the MMC, select the name of the Certification Authority (CA), and expand the view by clicking on the "+" sign.
- Select **Policy Settings** and make sure that the "Smartcard User" and "Enrollment Agent" items exist.

If they do not exist, select "New / Certificate to Issue" from the **Policy Settings** context menu.

In the **Certificate Template Selection** dialog, select "Smartcard User." Repeat this step to add the "Enrollment Agent" item.

Others maybe selected depending on your authentication requirements.

Set Certificate Template permissions.

- Select **Active Directory Sites and Services** in the MMC and ensure that the user or group of users issuing (enrolling) tokens have Read and Enroll permissions on the "Enrollment Agent" template.

The users or group of users who should be able to log on to Windows with their smart cards must have Read and Enroll permission on the "Smartcard User" template.

Create Enrollment Agent's Certificate

- Select **Certificates** in the MMC, expand Certificate - Current User, select **Personal** and select "Request Certificate " from the context menu. The certificate request wizard starts up.
- Select "Enrollment Agent," and then click **Next**.
- Enter a "friendly" certificate name, and then click **Finish**.

Issuing Logon Tokens

Initialize token

Tokens and smart cards need to be initialized, or formatted, before they can be used. Aladdin, for example, provides the eToken Pro Format utility as part of their Runtime Environment. The number of invalid PIN (password) entry attempts can be configured with this utility.

ProtectDrive imposes a one-minute lockout after three failed PIN entry attempts. Limiting the number of retries allowed for a token before it is locked will increase the overall security of the system.

Enroll the user

Refer to the Microsoft documentation for full details on configuring the Microsoft Certificate Services.

Typically, the certificate services are accessed via a Web browser by navigating to <http://COMPUTERNAME/certsrv/>, where COMPUTERNAME is the name of the server running the Microsoft CA.

- Select **Request a certificate**, and then click **Next**.
- Select **Advanced Request**, and then click **Next**.
- Select **Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station**, and then click **Next**.
- Set the **Certificate Template** to “Smartcard User.”

Note: With this option enabled, the certificate will be published in the Active Directory, allowing for the user to be added at install time.

- Select the Cryptographic Service Provider (CSP) (e.g., “eToken Base Cryptographic Provider”).
- Leave all other defaults as set, and then click **Enroll**.

Using Other Certificates for Pre-Boot Authentication

ProtectDrive can be configured to use certificates other than the Windows smart card logon certificate for pre-boot authentication. An administrator can define the required key usages and enhanced key usages during installation or post-installation via the Advanced Configuration application.

Certificates can be enrolled using the same procedure as described above. However, other certificate templates can be used to have greater control over the certificates accepted by ProtectDrive.

See [CHAPTER 6](#) and [CHAPTER 11](#) for details on these configuration options.

CHAPTER 20

The Multiple Boot System

Introduction

The ProtectDrive Multiple Boot system provides a method of management for more than one Windows operating system. ProtectDrive can be installed on any of these operating systems. Data security can be achieved by encrypting partitions, which then become exclusively owned by one of the installed operating systems.

Up to four bootable systems can be supported.

Limitations to Version 7.2.*

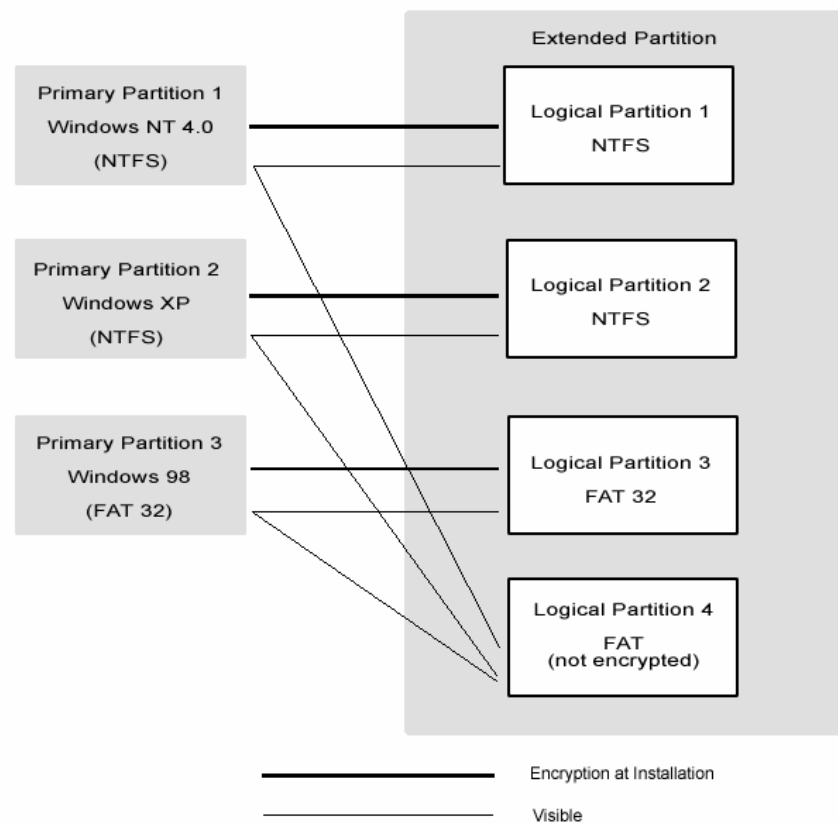
- Ensure that users are not Administrators. Although the contents of partitions belonging to companion boot-systems are hidden, administrators can format them from Windows Explorer.
- The boot systems must share the same registration disk.
- Only partitions on the first physical disk (i.e., with entries in the partition table in the master boot record) can be managed by the ProtectDrive Boot Manager.
- The upgrade from ProtectDrive multi-boot version 5.12.12 is not supported. This earlier version needs to be uninstalled before the current version can be installed.

Design Considerations

Users must be prepared to accept that multiple-booting arrangements have a level of complexity that requires some technical understanding of the concepts involved.

It is recommended that anyone unfamiliar with multiple booting should research Microsoft's Knowledge Database for tips on the multiple boot environment. The on-line Help section supplied with Windows 2000 under "Multiple Operating Systems" also contains relevant background information.

A ProtectDrive multi-boot system should be planned before starting installation. After the first installation of ProtectDrive, no further changes can be made to the partitions constituting the components of the file system. This includes slave hard drives.



Schematic of a typical multiple boot system

Warning: Earlier Windows operating systems were subject to hard drive boundaries (notably 2, 3.5 and 7.8 GB), some of which are analyzed in the Microsoft Knowledge database article Q 114841.

It is possible to infringe upon these restrictions when using imaging tools that often do not give warning messages.

Operating Systems

ProtectDrive Multiple Boot uses the Primary Partitions on the Primary Master hard drive. Since the DOS standard supports 1- 4 Primary Partitions up to four different Operating Systems can be installed.

However, the fourth Primary Partition is recommended to be kept as an Extended Partition to contain at least one Logical Partition to be associated with each Operating System installation. This will allow keeping user data separate from the system drive.

File Systems

ProtectDrive supports FAT16, FAT32, NTFS4, and NTFS5 file systems. When designing your system, bear in mind the limitations of earlier Windows operating systems to access the type of file system of partitions intended to be shared. For example, refer to Microsoft Knowledge Base article Q306559 for a post-release Windows XP summary.

Sharing Data

One or more additional Logical Partitions (not intended for encryption) may be made as a data exchange medium among the components of the multi-boot system, provided this does not compromise security.

Operating System Installation

ProtectDrive only installs if the system drive of the Operating System (OS) is designated as drive C. Thus, each OS must assign its system partition as drive letter C. This can be achieved by setting the partition the OS is being installed on as active, for example, by using `fdisk` or the Windows 2000 or XP Disk Management tool.

Note: The ProtectDrive Boot Manager is not compatible with the Windows Boot Manager, which is configured through the `boot.ini` system file. Setting a partition active before installing Windows and re-booting to a bootable Windows setup medium ensures that this file is not created. Alternatively, `boot.ini` can be manually edited to remove additional boot options.

Installation

Disk Management Tools

The disk management tools that are part of Windows 2000 and XP are highly recommended. Alternatively, *fdisk* can be used to create partitions and set them active as required.

Partitioning

It is important that all partitioning operations *must* be completed before ProtectDrive is installed, otherwise data that has not been backed up *will* be lost.

Initial partitioning can be accomplished using a third-party tool like Partition Magic. Otherwise, create a Primary Partition and install Windows 2000 or XP. Then use the Computer Management tool in Windows to create a second Primary Partition. The remaining space on the hard drive can be used to create an Extended Partition with any number of Logical Partitions. If Windows NT 4.0 is to be part of the final boot system, you can create its NTFS4 partition by this method using Administrative Tools.

Labeling Partitions

A useful tip to remember is to give the partitions meaningful labels. This will be of assistance when encrypting/decrypting, as ProtectDrive displays these labels when View or List is selected.

Another useful technique is to create partitions with slightly different sizes, noting size, label, and file system type. When descending to low-level tools like `fdisk`, the drive letter sequence can be different to that seen in Windows. This is sometimes the case in the Windows Setup utility when formatting a partition for the installing system to reside. Selecting an unwanted partition may result in lost data.

Other Operating Systems

Other operating systems, such as Linux, can be installed on the system and can be booted from the ProtectDrive boot menu. The same partition layout restrictions apply.

Notes:

- The Linux boot partition must be a primary partition; the other partitions, such as `/` and `swap`, can reside in an extended partition.
- Install the Linux Boot Manager *lilo* in the Linux boot partition.
- The installation of *lilo* in the Master Boot Record (MBR) is not supported, as this would conflict with the ProtectDrive Master Boot Loader (MBL) and protection system.

Pre-Installation Verification

After installing the required operating systems, successively mark each one **active**, then start it up. Verify that it is configured as required and that the partition is of the type that it is able to recognize.

Take special care to note if the active drive has been labeled C: ProtectDrive will not install if this is not the case.

Windows NT/2000/XP can be configured to run from a drive other than C. This has been observed, particularly in XP installations, where two or more multiple boot operating systems are XP.

Following are some remedies:

- Install on the target partition from the distribution medium, taking great care to nominate the correct partition and checking that it is actually labeled **C:**.
- Remove slave drives before installation as the first primary partition on the slave has been observed to interfere and usurp the C: name.
- If imaged, make the image from an installation in the correct position, such as the third primary partition.
- Refer to Microsoft Knowledge Base Article - Q223188
- Make sure the partition that ProtectDrive is going to be installed on is marked as active.

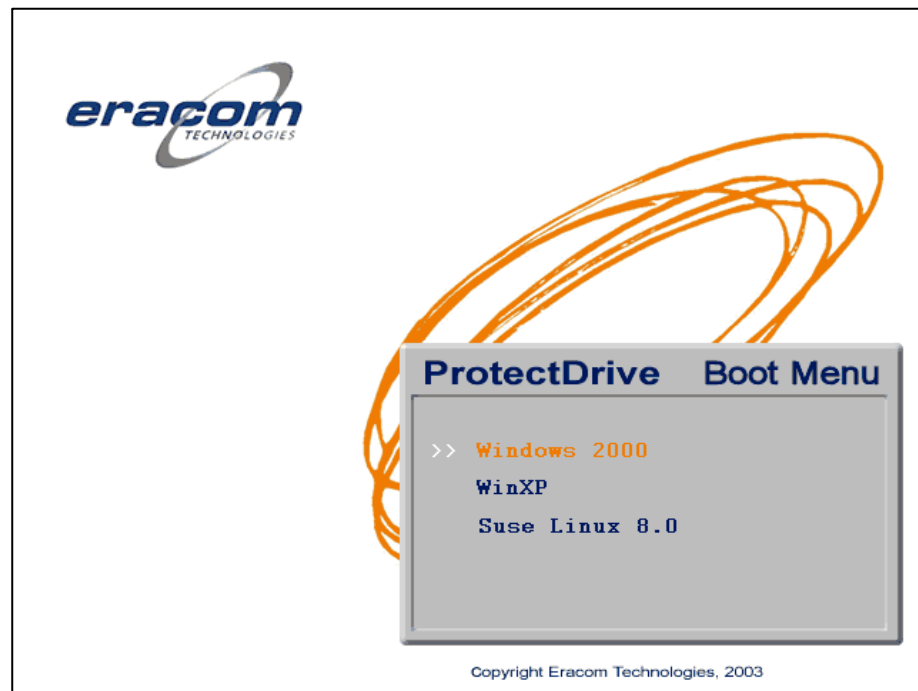
Notes:

- From this point on, no changes must be made to the partition layout of the disk.
- ProtectDrive Multi Boot Manager does not verify if the operating system is properly installed. If the partition is primary (not logical) and contains the signature value at the end of the boot sector, Multi Boot Manager will list the partition as bootable in its menu. The installer must verify that all Operating Systems are installed in the manner described in this document.

Installing

Install ProtectDrive on the *first* primary partition encrypting the C: drive and any Logical Partitions that are to be visible to the operating system on this partition.

After the first system is completed, the ProtectDrive multiple boot window will be displayed with a selection list from 1-4 corresponding to the number of Primary partitions defined.



Install ProtectDrive on the *second* and subsequent primary partitions encrypting the C: drive and any Logical Partitions that are to be visible to the operating system on the owning partition.

Notes:

- ProtectDrive does not have to be installed on other primary partitions. The convenience of having the functionality of other Windows operating systems can be exploited, provided that other data does not have to be completely secured. Remember that under the ProtectDrive multiple boot arrangement, all other primary partitions are hidden from the one selected at startup.
- ProtectDrive can only be installed on Windows NT, 2000, and XP.
- Encryption may be deferred until both or all operating systems have ProtectDrive installed, but any unencrypted logical partition will be fully visible to all operating systems.
- Partitions *not* visible to one or other operating system will be displayed in Windows Explorer with the label *Local Disk*. Clicking on these drives will result in an invitation to format them, which *must* be refused if the user is an Administrator, as the data cannot be recovered.
- After installation of Multi Boot Manager and encryption of required drives, create users *without* Administrator group privileges for subsequent general logging-on, as inadvertent formatting of hidden drives cannot then take place.

Uninstalling ProtectDrive

Uninstallation of ProtectDrive on individual operating system partitions follows the same procedure as described in CHAPTER 9.

However, the ProtectDrive boot menu will be removed with the last instance of ProtectDrive and will leave the system without a boot manager. The individual partitions can be booted by setting them active or the Windows boot manager can be activated by creating a corresponding boot.ini file that references all bootable partitions.

CHAPTER 21

ACS Error Messages and System Recovery

Error message identification

The ProtectDrive Access Control System (ACS) becomes active when a computer with ProtectDrive installed boots up. If an error occurs during its initialization, the system will display an error message composed of an error number and a brief description.

Error numbers are composed of three components:

CTXX where

C	is the module the error occurred in
T	identifies the type of error and
XX	is the actual error number

Module identifiers are:

0	Master Boot Loader (MBL)
1	VXBIOS
2	Not used
3	VROM

Type identifiers are:

0	Not used
1	Warning
2	Error
3	Fatal

The following table lists all ACS errors together with possible causes and recommended recovery action.

Note:

The Standard Recovery Procedure referred to in the table is described at the end of this chapter.

ACS Error	Component	Description	Possible cause	Recovery action
0301	MBL	Invalid master boot code checksum	MBR corruption MBR Trojan attack	Run RMBR.EXE to recover the ProtectDrive MBR.
0305	MBL	Invalid VXBIOS	Signature, checksum or size verification of the VXBIOS failed possibly caused by disk corruption	Contact Eracom Support
0306	MBL	Invalid master boot record signature	MBR corruption MBR Trojan attack	Run RMBR.EXE to recover the ProtectDrive MBR.
0307	MBL	No ERACOM partition info	Partition table corruption or change. Addition of fixed disk after ProtectDrive installation	Run RMBR.EXE to recover the ProtectDrive MBR.
0313	MBL	Disk i/o error reading sector stack	Disk IO error (Hard disk failure) or partition table corruption	Run RMBR.EXE to recover the ProtectDrive MBR.
0314	MBL	Disk i/o error reading VXBIOS	Disk IO error (Hard disk failure) or partition table corruption	Run RMBR.EXE to recover the ProtectDrive MBR.
1100	VXBIOS	System Not Initialised	System could not load the disk encryption key or the DTE EFS is missing or corrupted.	Standard Recovery Procedure
1204	VXBIOS	VROM load Error	VROM file is missing, has an incorrect size or a read error occurred	Standard Recovery Procedure
1205	VXBIOS	VROM Status Error	VROM signature verification failed or the program loader reported an error.	Standard Recovery Procedure
1300	VXBIOS	Insufficient memory	Failed to allocate memory for the VROM Insufficient memory available	Try to free up resources
1301	VXBIOS	GDA file load error	GDA file is missing or a read error occurred when trying to initialize encryption information	Standard Recovery Procedure
1310	VXBIOS	Cannot Init EFS	EFS corruption	Standard Recovery Procedure
1311	VXBIOS	VROM load Error	VROM file is missing, has an incorrect size or a read error occurred (Displayed after a ACS1204 error)	-
1312	VXBIOS	VXVECT save fail	Failed to store original disk interrupt service routine (ISR) address in the EFS super block EFS corruption	Standard Recovery Procedure
1313	VXBIOS	SBLK get fail	Failed to locate the EFS Super Block	Run RMBR.EXE to attempt to restore the ProtectDrive MBR

ACS Error	Component	Description	Possible cause	Recovery action
1314	VXBIOS	Info open fail	Missing VDX EFS file EFS corruption	Standard Recovery Procedure
1315	VXBIOS	Info write fail	EFS corruption	Standard Recovery Procedure
1316	VXBIOS	VROM EXEC fail	Failed to execute the VROM (Displayed after a ACS1205 error)	-
1317	VXBIOS	Info read fail	EFS corruption	Standard Recovery Procedure
1318	VXBIOS	Diskette boot fail	Master Boot Loader signature verification failed; Missing operating system on floppy disk	Use bootable floppy diskette; Eject floppy diskette from drive and boot from hard disk
1319	VXBIOS	GDA open fail	GDA file is missing when trying to load (and execute) the original MBL.	Standard Recovery Procedure
1320	VXBIOS	GDA read fail	A read error occurred on the GDA file when trying to load (and execute) the original MBL.	Standard Recovery Procedure
1321	VXBIOS	Boot fail	Master Boot Loader signature verification failed.	Standard Recovery Procedure
3301	VROM	Too many logon attempts	Forgotten password Corrupted user database	Log on as other user; Exercise user key recovery; Run DISPEFS.EXE
3302	VROM	I/O error reading disk	Corrupted EFS Hard disk failure	Standard Recovery Procedure
3304	VROM	An unknown error has occurred	Internal program error	Standard Recovery Procedure
3305	VROM	Configuration file has been corrupted	MAC check of configuration file failed Corrupted EFS	Standard Recovery Procedure
3306	VROM	User information has been corrupted	MAC check of user database entry failed Corrupted EFS	Log on as different user at pre-boot and let failed user log on to Windows. User database entry will be regenerated. Alternatively, exercise user key recovery mechanism.

ACS Error	Component	Description	Possible cause	Recovery action
3308	VROM	Built-in Administrator information has been corrupted	MAC check of built-in administrator failed; Corrupted EFS	Log on as different user at pre-boot and let failed user log on to Windows User database entry will be regenerated. Alternatively, exercise user key recovery mechanism.
3309	VROM	Configuration file has been fatally corrupted	EFS corruption Hard disk failure	Standard Recovery Procedure
3310	VROM	Error occurred initializing the token	The token module could not be initialized and password logons are not allowed.	To diagnose this error further contact Eracom. To get access to the system, exercise the token password fallback function.

Standard Recovery Procedure

The following procedure shows typical steps in recovering an unbootable system. It should be taken as a guide only and, if unsure, we recommend you contact Eracom support to assist with the recovery of your system. Details on the use of the ProtectDrive recovery tools can be found in CHAPTER 14.

Problem

Password type account user cannot be authenticated by the ProtectDrive Preboot Authentication program.

Smartcard/Token type account user cannot be authenticated by the ProtectDrive Pre-boot Authentication program.

User successfully authenticates at pre-boot, but Windows does not boot.

Fix

Run *Dispefs.exe /u*. This will display a list of all users and their account types. Password type account users are indicated with **Token User = False** setting.

If the user is shown to have a Password account type, then it is possible they are entering an invalid password. Passwords are case-sensitive. Finally, if the user is positive they are entering the correct password, and no other user is able to log on; then the ProtectDrive files have become corrupt. See below for *ProtectDrive appears to be corrupt*.

Run *Dispefs.exe /u*. to list of all existing users and their account types. Smartcard/Token type account users are designated with **Token User = True** setting.

Although a user may have one or more token accounts, it is possible that the Certificate contained by the token does not match the Certificate originally used for this user's record creation in the ProtectDrive Preboot User dB. The "Hash" field displayed by *Dispefs.exe /u* is the same as the "Thumbprint" field displayed when certificate details are viewed in Windows. Finally, if the user is positive they are using a valid token, and no other user is able to log on; then the ProtectDrive files have become corrupt. See below for *ProtectDrive appears to be corrupt*.

It is possible that one of the Windows system files is corrupt. If Drive **C** is not encrypted, proceed with normal Windows recovery. If Drive **C** is encrypted, run *Decdisk.exe* to enable Windows Recovery tools access the system drive.

ProtectDrive Pre-boot Authentication Program does not run.

If *fdisk /mbr* or another utility has replaced the ProtectDrive MBR the Preboot Authentication program will not be run.

If the system drive is encrypted the operating system will also fail to load.

If the system drive is not encrypted, but other drives are, the operating system will load but access to the encrypted drives will be prevented by the ProtectDrive driver.

To recover from this situation run *rmbr /p*.

ProtectDrive appears to be corrupt.

If ProtectDrive is corrupt; then one of the following is possible:

- 1 Preboot Authentication Program will not run or behaves strangely.
- 2 Valid users can not be authenticated at preboot.
- 3 Operating system fails to load.

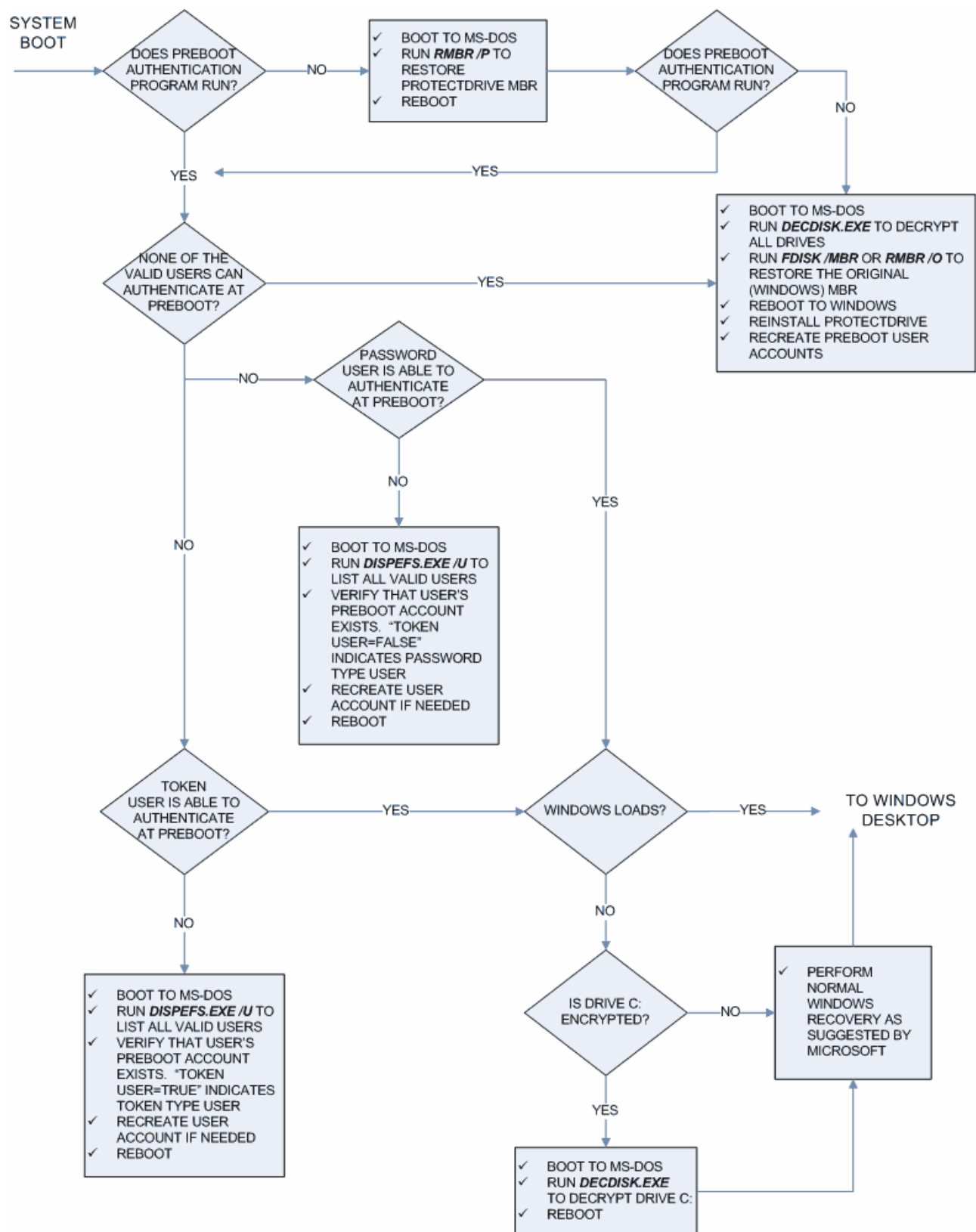
If none of the above sections apply, or you failed to restore ProtectDrive to normal working order, then all of the encrypted drives will need to be decrypted using *Decdisk.exe*.

If *Decdisk.exe* is unable to access the ProtectDrive Embedded File System (EFS); then use the Recovery Files originally created by *Backup.exe*.

Once all the drives have been decrypted, run *fdisk /mbr* or *rmbr /o* to restore the ProtectDrive MBR.

It is possible to boot the operating system once the system drive has been decrypted. It is not possible to uninstall ProtectDrive until all drives are decrypted.

The following flowchart represents the system debug information listed above. It is included for additional information.



THIS PAGE INTENTIONALLY LEFT BLANK

Technical Support

If you encounter a problem while installing, registering, or operating ProtectDrive, please make sure that you have read the relevant sections of this manual.

Should you still have problems that cannot be resolved, please contact Eracom support on the following numbers:

Within Australia: 1-800-634 796

Outside Australia: + 61 7 5593 4796

email: support@safenet-inc.com

Before contacting Eracom support, please ensure that you have the following information available:

- Version of product
- Support certificate number

END OF DOCUMENT